© 2022 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

**NOTE**

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.
Welcome to Veeam Backup for AWS

Integration with Veeam Backup & Replication

Planning and Preparation

Ports
AWS Services
IAM Permissions

Service IAM Role Permissions
Repository IAM Role Permissions
Policy IAM Role Permissions
Indexing IAM Role Permissions
Restore IAM Permissions
Full List of IAM Permissions
Considerations and Limitations

Licensing
Installing and Removing License
Viewing License Information
Revoking License Units

Architecture Overview

Deployment
Installing Veeam Backup for AWS from AWS Marketplace
After You Install
Installing Veeam Backup for AWS from AMI
Required IAM Permissions
After You Install
Uninstalling Veeam Backup for AWS
Deleting CloudFormation Stack
Deleting AWS Resources

Accessing Veeam Backup for AWS

Configuring Veeam Backup for AWS
Managing IAM Roles
Adding IAM Roles
Editing IAM Role Settings
Checking IAM Role Permissions
Removing IAM Roles
Managing Permissions ........................................................................................................ 120
Adding User Accounts .................................................................................................... 122
Editing User Account Settings ......................................................................................... 123
Changing User Passwords ............................................................................................... 124
Configuring Multi-Factor Authentication ......................................................................... 125
Managing Backup Repositories ....................................................................................... 127
Adding Backup Repositories ........................................................................................... 128
Editing Backup Repository Settings ................................................................................ 128
Removing Backup Repositories ....................................................................................... 129
Managing Worker Instances ......................................................................................... 140
Managing Worker Configurations .................................................................................. 141
Managing Worker Profiles .............................................................................................. 149
Configuring General Settings ......................................................................................... 153
Configuring Global Retention Settings .......................................................................... 154
Configuring Global Email Notification Settings ............................................................ 156
Replacing Security Certificates ....................................................................................... 159
Changing Time Zone ....................................................................................................... 161
Configuring SSO Settings ............................................................................................... 162
Performing Configuration Backup and Restore ............................................................... 164
Performing Configuration Backup Manually ................................................................... 165
Performing Configuration Backup Automatically ............................................................ 166
Exporting Configuration Backup Data ............................................................................. 167
Restoring Configuration Data ........................................................................................ 168

VIEWING AVAILABLE RESOURCES ....................................................................... 177
Adding Resources to Policy .............................................................................................. 178

PERFORMING BACKUP ......................................................................................... 179
How Backup Works ......................................................................................................... 181
EC2 Backup ....................................................................................................................... 182
RDS Backup ....................................................................................................................... 187
EFS Backup ......................................................................................................................... 189
VPC Configuration Backup ............................................................................................... 192
Retention Policy ................................................................................................................ 193
Performing EC2 Backup ................................................................................................... 199
Creating EC2 Backup Policies ......................................................................................... 200
Creating EC2 Snapshots Manually .................................................................................. 240
Performing RDS Backup ................................................................................................... 242
Creating RDS Backup Policies ........................................................................................ 243
Creating RDS Snapshots Manually .................................................................................. 267
Performing EFS Backup ................................................................................................... 269
Creating EFS Backup Policies ................................................................. 270
Creating EFS Backups Manually ................................................................ 299
Performing VPC Configuration Backup .................................................. 301
Editing VPC Configuration Backup Policy ............................................. 302
Enabling and Disabling VPC Configuration Backup Policy .................. 311
Starting and Stopping VPC Configuration Backup Policy ...................... 312
Managing EC2, RDS and EFS Backup Policies ........................................ 313
Starting and Stopping Policies ..................................................................... 314
Disabling and Enabling Policies .......................................................... 315
Setting Policy Priority .............................................................................. 316
Editing Policy Settings ............................................................................ 317
Exporting and Importing Policies .......................................................... 318

MANAGING BACKED-UP DATA.............................................................. 320
Managing Backed-Up EC2 Data ............................................................. 321
Removing EC2 Backups and Snapshots ................................................... 322
Removing EC2 Snapshots Created Manually ......................................... 323
Retrieving Data From Archive ............................................................... 324
Managing Backed-Up RDS Data ............................................................. 327
Removing RDS Snapshots ......................................................................... 328
Removing RDS Snapshots Created Manually ......................................... 329
Managing Backed-Up EFS Data ............................................................. 330
Removing EFS Backups ........................................................................... 331
Removing EFS Backups Created Manually ............................................ 332
Managing Backed-Up VPC Configuration Data ...................................... 333
Removing VPC Configuration Backups ................................................... 334
Comparing VPC Configuration Backups .................................................. 335
Exporting VPC Configuration ............................................................... 336

PERFORMING RESTORE ........................................................................ 352
EC2 Restore ............................................................................................. 353
Performing Entire EC2 Instance Restore ................................................... 354
Performing Volume-Level Restore ......................................................... 370
Performing File-Level Restore .............................................................. 385
RDS Restore ............................................................................................. 395
Step 1. Launch RDS Restore Wizard .......................................................... 396
Step 2. Select Restore Point ....................................................................... 397
Step 3. Specify IAM Identity ..................................................................... 398
Step 4. Choose Restore Mode .................................................................... 401
Step 5. Enable Encryption ........................................................................ 403
Step 6. Configure Restore Settings ......................................................... 404
Step 7. Configure Network Settings ................................................................. 410
Step 8. Specify Restore Reason ........................................................................... 412
Step 9. Finish Working with Wizard ................................................................. 413
EFS Restore ........................................................................................................ 414
Performing Entire File System Restore .......................................................... 415
Performing File-Level Restore ......................................................................... 428
VPC Configuration Restore .............................................................................. 444
Performing Entire Configuration Restore ....................................................... 445
Performing Selected Items Restore ................................................................. 456
ENABLING DATA ENCRYPTION.................................................................... 465
Backup Repository Encryption ........................................................................ 466
AWS KMS Encryption ....................................................................................... 467
Creating Cloud-Native Snapshots ................................................................. 468
Creating Snapshot Replicas ........................................................................... 469
Restoring From Snapshots and Replicas ....................................................... 473
Creating Image-Level Backups ......................................................................... 479
Restoring From Image-Level Backups ............................................................ 481
REVIEWING DASHBOARD............................................................................. 483
VIEWING SESSION STATISTICS .................................................................. 485
COLLECTING OBJECT PROPERTIES ............................................................... 486
UPDATING VEEAM BACKUP FOR AWS ...................................................... 487
Checking for Updates ....................................................................................... 488
Installing Updates ............................................................................................ 489
Updating IAM Roles ......................................................................................... 492
Viewing Updates History ................................................................................ 494
GETTING TECHNICAL SUPPORT ................................................................... 495
APPENDICES ................................................................................................. 497
Appendix A. Creating IAM Roles in AWS ....................................................... 498
Appendix B. Creating IAM Policies in AWS ..................................................... 500
Appendix C. Configuring Endpoints in AWS .................................................. 501
Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com
About This Document

This guide is intended for IT managers, cloud infrastructure administrators, and other personnel responsible for the product installation and operation.

The guide contains information on Veeam Backup for AWS configuration and provides a set of tasks that are required to perform data protection and disaster recovery operations.
Welcome to Veeam Backup for AWS

Veeam Backup for Amazon Web Services (Veeam Backup for AWS) is a solution developed for protection and disaster recovery tasks for Amazon Elastic Compute Cloud (EC2), Amazon Relational Database Service (RDS) and Amazon Elastic File System (EFS) environments. Veeam Backup for AWS also allows you to back up and restore Amazon Virtual Private Cloud (VPC) configurations.

**IMPORTANT**

Veeam Backup for AWS is available only in AWS Global and AWS GovCloud (US) regions.

With Veeam Backup for AWS, you can perform the following data protection operations:

- Create cloud-native snapshots of EC2 instances.
- Create cloud-native snapshots of RDS resources: DB instances and Amazon Aurora DB clusters (Aurora DB clusters).
- Replicate cloud-native snapshots to any AWS Region within any AWS account.
- Create image-level backups of EC2 instances and keep them in Amazon Simple Storage Service (Amazon S3) for high availability, cost-effective and long-term storage.
- Create backups of EFS file systems and store them in any backup vault in the source AWS Region.
- Create backup copies of EFS file systems and store them in any AWS Region within the same AWS account.
- Create backups of VPC configurations and keep them in the Veeam Backup for AWS database and in Amazon S3.
- Create backups of the Veeam Backup for AWS configuration database.

To recover backed-up data, you can perform the following operations:

- Restore entire EC2 instances.
- Restore EC2 instance volumes.
- Restore EC2 instance files and folders.
- Restore RDS DB instances and Aurora DB clusters.
- Restore entire EFS file systems.
- Restore EFS files and directories.
- Restore entire VPC configurations of AWS Regions.
- Restore specific items of VPC configurations of AWS Regions.
- Restore the Veeam Backup for AWS configuration database to the same or another backup appliance.
Integration with Veeam Backup & Replication

AWS Plug-in for Veeam Backup & Replication extends the Veeam Backup & Replication functionality and allows you to add Veeam Backup for AWS appliances into the Veeam Backup & Replication infrastructure. With AWS Plug-in for Veeam Backup & Replication, you can manage data protection and recovery operations from the Veeam Backup & Replication console. For more information, see the Integration with Veeam Backup & Replication Guide.

TIP
If you have multiple backup appliances in the AWS infrastructure, you can add the appliances to Veeam Backup & Replication, and then use the Veeam Backup & Replication console as the central management console for Veeam Backup for AWS operations. For more information on the Veeam Backup & Replication console, see the Veeam Backup & Replication User Guide.
Planning and Preparation

Before you start using Veeam Backup for AWS, consider the following requirements:

- Network ports that must be open to ensure proper communication of Veeam Backup for AWS components.
- AWS services to which Veeam Backup for AWS must have outbound internet access.
- IAM permissions that must be assigned to an IAM role or IAM user used to perform Veeam Backup for AWS operations.
- Considerations and limitations that should be kept in mind before you deploy Veeam Backup for AWS.
## Ports

The following network ports must be open to ensure proper communication of components in the Veeam Backup for AWS infrastructure.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser (local machine)</td>
<td>Backup appliance</td>
<td>TCP</td>
<td>443</td>
<td>Required to access the Web UI component from a user workstation.</td>
</tr>
<tr>
<td>SSH</td>
<td>Backup appliance</td>
<td>TCP</td>
<td>22</td>
<td>Required to communicate with the backup service running on the backup appliance.</td>
</tr>
<tr>
<td>TCP</td>
<td>Backup appliance</td>
<td>11005</td>
<td>Default port required to communicate with the REST API service running on the backup appliance.</td>
<td></td>
</tr>
<tr>
<td>To learn how to change the port number, see the Configuring Security Settings section in the Veeam Backup for AWS REST API Reference.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Worker instance</td>
<td>TCP</td>
<td>443</td>
<td>Required to access the file-level recovery browser running on a worker instance during the file-level restore process.</td>
<td></td>
</tr>
<tr>
<td>Backup appliance</td>
<td>SMTP server</td>
<td>TCP</td>
<td>25</td>
<td>Default port used for sending email notifications.</td>
</tr>
<tr>
<td>Veeam Update Notification Server (repository.veeam.com)</td>
<td>TCP</td>
<td>443</td>
<td>Required to download information on available product updates.</td>
<td></td>
</tr>
</tbody>
</table>

To open network ports, you must add inbound rules to security groups associated with Veeam Backup for AWS infrastructure components:

- A security group for the backup appliance is created during the product installation. For more information, see Installing Veeam Backup for AWS from AWS Marketplace and Installing Veeam Backup for AWS from AMI.

- A security group for worker instances is selected per AWS Region and Availability Zone. For more information, see Configuring Worker Instance Settings.

To learn how to add inbound rules to security groups, see AWS Documentation.
The backup appliance and worker instances must have outbound internet access to the following AWS services:

- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Kinesis Data Streams
- Amazon Relational Database Service (RDS)
- Amazon Elastic File System (EFS)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Marketplace Metering Service
- AWS Resource Access Manager
- AWS Security Token Service (STS)
- AWS Service Quotas
- AWS Backup
- AWS Systems Manager (SSM), including access to the `ec2messages` and `ssmmessages` endpoints
- Elastic Load Balancing (ELB)
IAM Permissions

To perform data protection and disaster recovery operations, you must specify IAM roles and IAM users whose permissions Veeam Backup for AWS will use to access AWS services and resources.

When you deploy Veeam Backup for AWS, the Default Backup Restore IAM role is automatically created and added to the backup appliance. This IAM role is assigned all permissions required to perform operations in the same AWS account where the backup appliance resides. However, you can create additional IAM roles to perform operations in this or in other AWS accounts. To learn how to create IAM roles and assign them the required permissions, see Appendix A. Creating IAM Roles in AWS.

For more information on IAM roles in Veeam Backup for AWS, see Managing IAM Roles.
Service IAM Role Permissions

To allow Veeam Backup for AWS to launch worker instances in the backup account to perform backup and restore operations, the Service IAM role specified in the worker instance settings must be granted the following permissions:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ec2:AttachVolume",
                "ec2:CopySnapshot",
                "ec2:CreateKeyPair",
                "ec2:CreateSnapshot",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteKeyPair",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeInstances",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:ModifyInstanceAttribute",
                "ec2:ModifySnapshotAttribute",
                "ec2:ModifyVolume",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "iam:AddRoleToInstanceProfile",
                "iam:AttachRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:CreateRole",
                "iam:DeleteInstanceProfile",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetContextKeysForPrincipalPolicy",
                "iam:GetInstanceProfile",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
            ]
        }
    ]
}
"iam:PassRole",
"iam:PutRolePolicy",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"kinesis:CreateStream",
"kinesis:DeleteStream",
"kinesis:DescribeStream",
"kinesis:PutRecord",
"kms:CreateGrant",
"kms:DescribeKey",
"kms:GenerateDataKeyWithoutPlaintext",
"kms:GetKeyPolicy",
"kms:ListAliases",
"kms:ListKeys",
"kms:ReEncryptFrom",
"kms:ReEncryptTo",
"servicequotas:ListServiceQuotas",
"sqs:CreateQueue",
"sqs:DeleteMessage",
"sqs:DeleteQueue",
"sqs:ListQueues",
"sqs:ReceiveMessage",
"sqs:SendMessage",
"ssm:GetCommandInvocation",
"ssm:GetParameter",
"ssm:SendCommand"
]

"Resource": "*"
}
Repository IAM Role Permissions

To allow Veeam Backup for AWS to create backup repositories in an Amazon S3 bucket and to access the repository when performing backup and restore operations, IAM roles specified in the repository settings must be granted the following permissions:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject", "s3:RestoreObject"],
            "Resource": "arn:aws:s3:::<yourbucketname>/*"
        },
        {
            "Effect": "Allow",
            "Action": ["s3:ListBucket", "s3:GetBucketLocation"],
            "Resource": "arn:aws:s3:::<yourbucketname>"
        },
        {
            "Effect": "Allow",
            "Action": ["ec2:DescribeRegions", "iam:GetContextKeysForPrincipalPolicy", "iam:SimulatePrincipalPolicy", "s3:ListAllMyBuckets"],
            "Resource": "*"
        }
    ]
}
```
To encrypt data stored in backup repositories using AWS KMS keys, IAM roles used to create the backup repositories must be granted the following permissions:

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:ListAliases",
        "kms:ListKeys"
    ],
    "Resource": "*"
}
```

**IMPORTANT**

If you plan to use KMS key encryption for backup repositories, consider the following:

- The key policy of an AWS KMS key that will be used to encrypt a repository must allow the IAM role specified in the repository settings access to the key.
- AWS managed keys cannot be used to encrypt repositories due to AWS limitations.
Policy IAM Role Permissions

To allow Veeam Backup for AWS to perform backup operations, IAM roles specified in the backup policy settings must be granted specific permissions that depend on AWS resources being backed up:

- EC2 Backup IAM Role Permissions
- RDS Backup IAM Role Permissions
- EFS Backup IAM Role Permissions
- VPC Configuration Backup IAM Role Permissions

EC2 Backup IAM Role Permissions

Veeam Backup for AWS uses EC2 Backup Policy IAM roles to perform the following operations:

- To enumerate resources added to a backup policy.
- To create cloud-native snapshots of EC2 instances protected by the policy.
- To create EBS volumes and attaching the volumes to worker instances when performing image-level backup.
- To create snapshot replicas, and so on.
To perform these operations, IAM roles specified in the backup policy settings must be granted the following permissions:
"Version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "ebs:ListChangedBlocks",
      "ebs:ListSnapshotBlocks",
      "ec2:CopySnapshot",
      "ec2:CreateSnapshot",
      "ec2:CreateSnapshots",
      "ec2:CreateTags",
      "ec2:DeleteSnapshot",
      "ec2:DeleteTags",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeConversionTasks",
      "ec2:DescribeImages",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeRegions",
      "ec2:DescribeSnapshotAttribute",
      "ec2:DescribeSnapshots",
      "ec2:DescribeSubnets",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeVolumes",
      "ec2:GetEbsDefaultKmsKeyId",
      "ec2:ModifySnapshotAttribute",
      "events:DeleteRule",
      "events:DescribeRule",
      "events:ListTargetsByRule",
      "events:PutRule",
      "events:PutTargets",
      "events:RemoveTargets",
      "iam:GetContextKeysForPrincipalPolicy",
      "iam:ListAccountAliases",
      "iam:ListInstanceProfiles",
      "iam:SimulatePrincipalPolicy",
      "kms:CreateGrant",
      "kms:DescribeKey",
      "kms:GetKeyPolicy",
      "kms:ListAliases",
      "kms:ListKeys",
      "kms:ReEncryptFrom",
      "kms:ReEncryptTo",
      "servicequotas:ListServiceQuotas",
      "sns:CreateTopic",
      "sns:DeleteTopic",
      "sns:ListSubscriptionsByTopic",
      "sns:ListTopics",
      "sns:SetTopicAttributes",
      "sns:Subscribe",
      "sns:Unsubscribe",
      "sqs:CreateQueue",
    ]
  }
]
RDS Backup IAM Role Permissions

Veeam Backup for AWS uses *RDS Backup Policy* IAM roles to perform the following operations:

- To enumerate resources added to a backup policy.
- To create cloud-native snapshots of RDS resources protected by the policy.
- To create snapshot replicas, and so on.
To perform these operations, IAM roles specified in the backup policy settings must be granted the following permissions:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:ListTargetsByRule",
                "events:PutRule",
                "events:PutTargets",
                "events:RemoveTargets",
                "iam:GetContextKeysForPrincipalPolicy",
                "iam:GetRole",
                "iam:SimulatePrincipalPolicy",
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GetKeyPolicy",
                "kms:ListAliases",
                "kms:ListKeys",
                "rds:AddTagsToResource",
                "rds:CopyDBClusterSnapshot",
                "rds:CopyDBSnapshot",
                "rds:CreateDBClusterSnapshot",
                "rds:CreateDBSnapshot",
                "rds:DeleteDBClusterSnapshot",
                "rds:DeleteDBSnapshot",
                "rds:DescribeDBClusters",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBInstances",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:ListTagsForResource",
                "rds:ModifyDBClusterSnapshotAttribute",
                "rds:ModifyDBSnapshotAttribute",
                "rds:RemoveTagsFromResource",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListSubscriptionsByTopic",
                "sns:ListTopics",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Unsubscribe",
                "sqs:CreateQueue",
                "sqs:DeleteMessage",
                "sqs:DeleteQueue",
                "sqs:ListQueues",
                "sqs:ReceiveMessage",
                "sqs:SendMessage",
                "sqs:SetQueueAttributes"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
EFS Backup IAM Role Permissions

Veeam Backup for AWS uses *EFS Backup Policy* IAM roles to perform the following operations:

- To enumerate resources added to a backup policy.
- To create EFS backups of file systems protected by the policy.
- To create backup copies, and so on.

To perform these operations, IAM roles specified in the backup policy settings must meet the following requirements:

1. The AWS Backup service must be granted permissions to assume the IAM roles.

   To allow the AWS Backup service to assume an IAM role, configure trusted relationships for the role and add the following statement to the trusted policy.

   ```json
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "sts:AssumeRole",
               "Principal": {
                   "Service": "backup.amazonaws.com"
               }
           }
       ]
   }
   ```

   To learn how to configure trusted relationships, see Appendix A. Creating IAM Roles in AWS.
2. The IAM roles must be granted the following permissions:
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "backup:CopyFromBackupVault",
        "backup:CopyIntoBackupVault",
        "backup:DeleteRecoveryPoint",
        "backup:DescribeBackupJob",
        "backup:DescribeCopyJob",
        "backup:DescribeRecoveryPoint",
        "backup:ListBackupVaults",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListTags",
        "backup:StartBackupJob",
        "backup:StartCopyJob",
        "backup:StopBackupJob",
        "backup:TagResource",
        "backup:UntagResource",
        "ec2:CreateKeyPair",
        "ec2:DeleteKeyPair",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:ListTagsForResource",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "iam:GetInstanceProfile",
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:ListAccountAliases",
      ]
    }
  ]
}
"iam:ListInstanceProfilesForRole",
"iam:PassRole",
"iam:SimulatePrincipalPolicy",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:ListSubscriptionsByTopic",
"sns:ListTopics",
"sns:SetTopicAttributes",
"sns:Subscribe",
"sns:Unsubscribe",
"sqs:CreateQueue",
"sqs:DeleteMessage",
"sqs:DeleteQueue",
"sqs:ListQueues",
"sqs:ReceiveMessage",
"sqs:SetQueueAttributes",
"ssm:GetCommandInvocation",
"ssm:GetParameter",
"ssm:SendCommand"
],
"Resource": "*",
"Effect": "Allow"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:TerminateInstances",
    "ec2:StartInstances"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "ec2:ResourceTag/EfsIndexWorker": "EfsIndexWorker"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "ec2:CreateAction": "RunInstances",
      "aws:RequestTag/EfsIndexWorker": "EfsIndexWorker"
    }
  }
}
VPC Configuration Backup IAM Role Permissions

Veeam Backup for AWS uses *VPC Configuration Backup Policy* IAM roles to perform the following operations:

- To enumerate resources added to a backup policy.
- To create VPC configuration backups of AWS Regions protected by the policy.
- To create backup copies, and so on.
To perform these operations, IAM roles specified in the backup policy settings must be granted the following permissions:
"Action": [
    "ec2:DescribeAddresses",
    "ec2:DescribeClientVpnAuthorizationRules",
    "ec2:DescribeClientVpnEndpoints",
    "ec2:DescribeClientVpnRoutes",
    "ec2:DescribeClientVpnTargetNetworks",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayMulticastDomains",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayPrefixListReferences",
    "ec2:GetTransitGatewayRouteTableAssociations",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "iam:GetContextKeysForPrincipalPolicy",
    "iam:ListAccountAliases",
    "iam:SimulatePrincipalPolicy",
    "ram:GetResourceShares",
    "ram:ListPrincipals",
    "ram:ListResources",
    "ram:ListResourceSharePermissions"
]
"Resource": "*",
"Effect": "Allow"
}
Indexing IAM Role Permissions

When performing EFS indexing operations, Veeam Backup for AWS launches worker instances in the same AWS account where file systems processed by backup policies belong. To communicate with these instances, Veeam Backup for AWS attaches to the instances *indexing IAM roles*. To learn how EFS indexing works, see *EFS Backup*.

By default, Veeam Backup for AWS selects the most appropriate network settings of AWS Regions in production accounts to launch worker instances. However, you can add worker configurations to specify network settings for each VPC in which worker instances will be deployed. When creating new worker configurations, Veeam Backup for AWS uses *Worker Configuration IAM roles* only to list network settings available in AWS Regions of production AWS accounts. To learn how to add worker configurations for indexing operations, see *Adding Configurations for Production Accounts*.

### Indexing IAM Role Permissions

To allow Veeam Backup for AWS to create indexes of the backed up EFS file systems, IAM roles specified in the *EFS backup policy settings* must be included at least in one instance profile and must meet the following requirements:

1. The Amazon EC2 service must be granted permissions to assume the IAM roles.

   To allow the Amazon EC2 service to assume an IAM role, configure trusted relationships for the role and add the following statement to the trusted policy.

   ```json
   ```

   To learn how to configure trusted relationships, see *Appendix A. Creating IAM Roles in AWS*.
2. The IAM roles must be granted the following permissions:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:ListAccountAliases",
        "iam:ListInstanceProfilesForRole",
        "iam:SimulatePrincipalPolicy",
        "ssm:DescribeAssociation",
        "ssm:DescribeDocument",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:PutInventory",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "sts:AssumeRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```
Worker Configuration IAM Role Permissions

If you add specific worker configurations that will be used for EFS indexing operations, consider that IAM roles specified in the worker configuration settings must be granted the following permissions:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```
To allow Veeam Backup for AWS to perform restore operations, IAM roles and IAM users whose one-time access keys are specified in the restore settings must have specific permissions that depend on AWS resources being restored:

- EC2 Restore IAM Permissions
- RDS Restore IAM Permissions
- EFS Restore IAM Permissions
- VPC Configuration Restore IAM Permissions
EC2 Restore IAM Permissions

To perform EC2 restore operations, IAM roles and IAM users specified in the restore settings must be granted the following permissions:
{ "Version": "2012-10-17",
"Statement": [
{
"Action": [
"ec2:AttachVolume",
"ec2:CopySnapshot",
"ec2:CreateKeyPair",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:DeleteKeyPair",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteVolume",
"ec2:DeregisterImage",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeImages",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeKeyPairs",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcs",
"ec2:DetachVolume",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:ImportImage",
"ec2:ModifyInstanceAttribute",
"ec2:ModifySnapshotAttribute",
"ec2:ModifyVolume",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"events:DeleteRule",
"events:DescribeRule",
"events:ListTargetsByRule",
"events:PutRule",
"events:PutTargets",
"events:RemoveTargets",
"iam:AddRoleToInstanceProfile",
"iam:AttachRolePolicy",
"iam:CreateInstanceProfile",
"iam:DeleteInstanceProfile",
"iam:DeleteRolePolicy",
"iam:DetachRolePolicy",
]
"iam:GetContextKeysForPrincipalPolicy",
"iam:GetInstanceProfile",
"iam:GetRole",
"iam:GetAttachedRolePolicies",
"iam:GetInstanceProfilesForRole",
"iam:GetRolePolicies",
"iam:PassRole",
"iam:PutRolePolicy",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"kms:CreateGrant",
"kms:DescribeKey",
"kms:GetKeyPolicy",
"kms:ListAliases",
"kms:ListKeys",
"kms:ReEncryptFrom",
"kms:ReEncryptTo",
"s3:GetBucketLocation",
"servicequotas:ListServiceQuotas"
},
"Resource": "*",
"Effect": "Allow"}
RDS Restore IAM Permissions

To perform RDS restore operations, IAM roles and IAM users specified in the restore settings must be granted the following permissions:
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "iam:CreateServiceLinkedRole",
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:ListAccountAliases",
        "iam:PassRole",
        "iam:SimulatePrincipalPolicy",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBSnapshot",
        "rds:CreateDBInstance",
        "rds:DeleteDBCluster",
        "rds:DeleteDbclusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSnapshot",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBSnapshotAttribute",
      ]
    }
  ]
}
EFS Restore IAM Permissions

To perform EFS restore operations, IAM roles and IAM users must be granted specific permissions.

IAM Role Permissions

IAM roles specified in the restore settings must meet the following requirements:

1. The AWS Backup service must be granted permissions to assume the IAM roles.

To allow the AWS Backup service to assume an IAM role, configure trusted relationships for the role and add the following statement to the trusted policy.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "Service": "backup.amazonaws.com"
            }
        }
    ]
}
```

To learn how to configure trusted relationships, see Appendix A. Creating IAM Roles in AWS.
2. The IAM roles must be granted the following permissions:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "backup:CopyFromBackupVault",
                "backup:CopyIntoBackupVault",
                "backup:CreateBackupVault",
                "backup:DeleteBackupVault",
                "backup:DeleteRecoveryPoint",
                "backup:DescribeCopyJob",
                "backup:DescribeRecoveryPoint",
                "backup:DescribeRestoreJob",
                "backup:ListTags",
                "backup:StartCopyJob",
                "backup:StartRestoreJob",
                "backup:TagResource",
                "backup-storage:MountCapsule",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "elasticfilesystem:CreateAccessPoint",
                "elasticfilesystem:CreateFileSystem",
                "elasticfilesystem:CreateMountTarget",
                "elasticfilesystem:DeleteAccessPoint",
                "elasticfilesystem:DeleteFileSystem",
                "elasticfilesystem:DeleteMountTarget",
                "elasticfilesystem:DescribeAccessPoints",
                "elasticfilesystem:DescribeFileSystemPolicy",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeMountTargetSecurityGroups",
                "elasticfilesystem:PutBackupPolicy",
                "elasticfilesystem:PutFileSystemPolicy",
                "elasticfilesystem:PutLifecycleConfiguration",
                "elasticfilesystem:Restore",
                "elasticfilesystem:TagResource",
                "elasticfilesystem:UntagResource",
                "elasticfilesystem:UpdateFileSystem",
                "iam:GetContextKeysForPrincipalPolicy",
                "iam:GetRole",
                "iam:GetAccountAliases",
                "iam:PassRole",
                "iam:SimulatePrincipalPolicy",
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ListAccountAliases",
                "kms:ListKeys"
            ]
        }
    ]
}
"Resource": "*",
"Effect": "Allow"
]}
}
}
IAM User Permissions

IAM users whose one-time access keys are specified in the restore settings must have the following permissions:
"elasticfilesystem:PutBackupPolicy",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:UpdateFileSystem"
],
  "Resource": "*",
  "Effect": "Allow"
}
VPC Configuration Restore IAM Permissions

To perform VPC configuration restore operations, IAM roles and IAM users specified in the restore settings must be granted the following permissions:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AcceptVpcEndpointConnections",
                "ec2:AllocateAddress",
                "ec2:AssociateAddress",
                "ec2:AssociateClientVpnTargetNetwork",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateTransitGatewayMulticastDomain",
                "ec2:AssociateTransitGatewayRouteTable",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachInternetGateway",
                "ec2:AttachVpnGateway",
                "ec2:AuthorizeClientVpnIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateClientVpnEndpoint",
                "ec2:CreateClientVpnRoute",
                "ec2:CreateCustomerGateway",
                "ec2:CreateDefaultSubnet",
                "ec2:CreateDefaultVpc",
                "ec2:CreateDhcpOptions",
                "ec2:CreateEgressOnlyInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:CreateManagedPrefixList",
                "ec2:CreateNatGateway",
                "ec2:CreateNetworkAcl",
                "ec2:CreateNetworkAclEntry",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateTransitGateway",
                "ec2:CreateTransitGatewayMulticastDomain",
                "ec2:CreateTransitGatewayPeeringAttachment",
                "ec2:CreateTransitGatewayPrefixListReference",
                "ec2:CreateTransitGatewayRoute",
                "ec2:CreateTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayVpcAttachment",
                "ec2:CreateVpc",
                "ec2:CreateVpcEndpoint",
                "ec2:CreateVpcEndpointServiceConfiguration",
                "ec2:CreateVpnConnection",
                "ec2:CreateVpnGateway",
                "ec2:DeleteClientVpnEndpoint",
                "ec2:DeleteClientVpnRoute",
                "ec2:DeleteCustomerGateway",
            ]
        }
    ]
}
"ec2:DeleteDhcpOptions",
"ec2:DeleteEgressOnlyInternetGateway",
"ec2:DeleteInternetGateway",
"ec2:DeleteManagedPrefixList",
"ec2:DeleteNatGateway",
"ec2:DeleteNetworkAcl",
"ec2:DeleteNetworkAclEntry",
"ec2:DeleteNetworkInterface",
"ec2:DeleteRoute",
"ec2:DeleteRouteTable",
"ec2:DeleteSecurityGroup",
"ec2:DeleteSubnet",
"ec2:DeleteTransitGateway",
"ec2:DeleteTransitGatewayMulticastDomain",
"ec2:DeleteTransitGatewayPeeringAttachment",
"ec2:DeleteTransitGatewayPrefixListReference",
"ec2:DeleteTransitGatewayRoute",
"ec2:DeleteTransitGatewayRouteTable",
"ec2:DeleteTransitGatewayVpcAttachment",
"ec2:DeleteVpc",
"ec2:DeleteVpcEndpoints",
"ec2:DeleteVpcEndpointServiceConfigurations",
"ec2:DeleteVpcPeeringConnection",
"ec2:DeleteVpnConnection",
"ec2:DeleteVpnGateway",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeClientVpnAuthorizationRules",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeClientVpnRoutes",
"ec2:DescribeClientVpnTargetNetworks",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPeeringAttachments",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs"
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DetachInternetGateway",
"ec2:DetachVpnGateway",
"ec2:DisableTransitGatewayRouteTablePropagation",
"ec2:DisableVgwRoutePropagation",
"ec2:DisassociateAddress",
"ec2:DisassociateClientVpnTargetNetwork",
"ec2:DisassociateRouteTable",
"ec2:DisassociateTransitGatewayMulticastDomain",
"ec2:DisassociateTransitGatewayRouteTable",
"ec2:EnableTransitGatewayRouteTablePropagation",
"ec2:EnableVgwRoutePropagation",
"ec2:GetManagedPrefixListEntries",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:ModifyClientVpnEndpoint",
"ec2:ModifyManagedPrefixList",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySubnetAttribute",
"ec2:ModifyTransitGateway",
"ec2:ModifyTransitGatewayVpcAttachment",
"ec2:ModifyVpcAttribute",
"ec2:ModifyVpcEndpoint",
"ec2:ModifyVpcEndpointServiceConfiguration",
"ec2:ModifyVpcPeeringConnectionOptions",
"ec2:ModifyVpnConnection",
"ec2:RejectVpcEndpointConnections",
"ec2:ReleaseAddress",
"ec2:ReplaceNetworkAclAssociation",
"ec2:ReplaceRouteTableAssociation",
"ec2:RevokeClientVpnIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:SearchTransitGatewayRoutes",
"elasticloadbalancing:AddTags",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:CreateTargetGroup",
"elasticloadbalancing:DeleteListener",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:DeleteTargetGroup",
"elasticloadbalancing:DeregisterTargets",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:ModifyTargetGroup",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:RemoveTags",
"elasticloadbalancing:SetSecurityGroups"
"elasticloadbalancing:SetSubnets",
"iam:GetContextKeysForPrincipalPolicy",
"iam:SimulatePrincipalPolicy",
"lambda:ListFunctions",
"ram:AssociateResourceShare",
"ram:CreateResourceShare",
"ram:DeleteResourceShare",
"ram:DisassociateResourceShare",
"ram:GetResourceShareAssociations",
"ram:GetResourceShares",
"ram:ListPrincipals",
"ram:ListResources",
"ram:ListResourceSharePermissions",
"ram:TagResource",
"ram:UntagResource",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:PutObject",
"servicequotas:ListServiceQuotas"
],
   "Resource": "*",
   "Effect": "Allow"
}
Full List of IAM Permissions

If you want Veeam Backup for AWS to use a single IAM role to perform all restore and backup operations, you can use the Default Backup Restore IAM role created during Veeam Backup for AWS installation or a custom IAM role that must be granted the following permissions:
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSnapshot",
"ec2:CreateSnapshots",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateTransitGateway",
"ec2:CreateTransitGatewayMulticastDomain",
"ec2:CreateTransitGatewayPeeringAttachment",
"ec2:CreateTransitGatewayPrefixListReference",
"ec2:CreateTransitGatewayRoute",
"ec2:CreateTransitGatewayRouteTable",
"ec2:CreateTransitGatewayVpcAttachment",
"ec2:CreateVolume",
"ec2:CreateVpc",
"ec2:CreateVpcEndpoint",
"ec2:CreateVpcEndpointServiceConfiguration",
"ec2:CreateVpcPeeringConnection",
"ec2:CreateVpnConnection",
"ec2:CreateVpnGateway",
"ec2:DeleteClientVpnEndpoint",
"ec2:DeleteClientVpnRoute",
"ec2:DeleteCustomerGateway",
"ec2:DeleteDhcpOptions",
"ec2:DeleteEgressOnlyInternetGateway",
"ec2:DeleteInternetGateway",
"ec2:DeleteKeyPair",
"ec2:DeleteManagedPrefixList",
"ec2:DeleteNatGateway",
"ec2:DeleteNetworkAcl",
"ec2:DeleteNetworkAclEntry",
"ec2:DeleteNetworkInterface",
"ec2:DeleteRoute",
"ec2:DeleteRouteTable",
"ec2:DeleteSecurityGroup",
"ec2:DeleteSnapshot",
"ec2:DeleteSubnet",
"ec2:DeleteTags",
"ec2:DeleteTransitGateway",
"ec2:DeleteTransitGatewayMulticastDomain",
"ec2:DeleteTransitGatewayPeeringAttachment",
"ec2:DeleteTransitGatewayPrefixListReference",
"ec2:DeleteTransitGatewayRoute",
"ec2:DeleteTransitGatewayRouteTable",
"ec2:DeleteTransitGatewayVpcAttachment",
"ec2:DeleteVolume",
"ec2:DeleteVpc",
"ec2:DeleteVpcEndpoints",
"ec2:DeleteVpcEndpointServiceConfigurations",
"ec2:DeleteVpcPeeringConnection",
"ec2:DeleteVpnConnection",
"ec2:DeleteVpnGateway",
"ec2:DescribeAccountAttributes",
"ec2:DescribeAddresses",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeClientVpnAuthorizationRules",
"ec2:DescribeClientVpnEndpoints",
"ec2:DescribeClientVpnRoutes",
"ec2:DescribeClientVpnTargetNetworks",
"ec2:DescribeConversionTasks",
"ec2:DescribeCustomerGateways",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeImages",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeInstanceTypes",
"ec2:DescribeInternetGateways",
"ec2:DescribeKeyPairs",
"ec2:DescribeLaunchTemplates",
"ec2:DescribeManagedPrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayAttachments",
"ec2:DescribeTransitGatewayMulticastDomains",
"ec2:DescribeTransitGatewayPeeringAttachments",
"ec2:DescribeTransitGatewayRouteTables",
"ec2:DescribeTransitGateways",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeVolumeAttribute",
"ec2:DescribeVolumes",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ec2:DetachInternetGateway",
"ec2:DetachVolume",
"ec2:DetachVpnGateway",
"ec2:DisableTransitGatewayRouteTablePropagation",
"ec2:DisableVgwRoutePropagation",
"ec2:DisassociateAddress",
"ec2:DisassociateClientVpnTargetNetwork",
"ec2:DisassociateRouteTable",
"ec2:DisassociateTransitGatewayMulticastDomain",
"ec2:DisassociateTransitGatewayRouteTable",
"ec2:EnableTransitGatewayRouteTablePropagation"
"ec2:EnableVgwRoutePropagation",
"ec2:GetEbsDefaultKmsKeyId",
"ec2:GetManagedPrefixListEntries",
"ec2:GetTransitGatewayMulticastDomainAssociations",
"ec2:GetTransitGatewayPrefixListReferences",
"ec2:GetTransitGatewayRouteTableAssociations",
"ec2:GetTransitGatewayRouteTablePropagations",
"ec2:ModifyClientVpnEndpoint",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyManagedPrefixList",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySnapshotAttribute",
"ec2:ModifySubnetAttribute",
"ec2:ModifyTransitGateway",
"ec2:ModifyTransitGatewayVpcAttachment",
"ec2:ModifyVolume",
"ec2:ModifyVpcAttribute",
"ec2:ModifyVpcEndpoint",
"ec2:ModifyVpcEndpointServiceConfiguration",
"ec2:ModifyVpcPeeringConnectionOptions",
"ec2:ModifyVpnConnection",
"ec2:RejectVpcEndpointConnections",
"ec2:ReleaseAddress",
"ec2:ReplaceNetworkAclAssociation",
"ec2:ReplaceRouteTableAssociation",
"ec2:RevokeClientVpnIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:RunInstances",
"ec2:SearchTransitGatewayRoutes",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"ec2messages:AcknowledgeMessage",
"ec2messages:DeleteMessage",
"ec2messages:FailMessage",
"ec2messages:GetEndpoint",
"ec2messages:GetMessages",
"ec2messages:SendReply",
"elasticfilesystem:Backup",
"elasticfilesystem:CreateAccessPoint",
"elasticfilesystem:CreateFileSystem",
"elasticfilesystem:CreateMountTarget",
"elasticfilesystem:DeleteAccessPoint",
"elasticfilesystem:DeleteFileSystem",
"elasticfilesystem:DeleteMountTarget",
"elasticfilesystem:DescribeAccessPoints",
"elasticfilesystem:DescribeBackupPolicy",
"elasticfilesystem:DescribeFileSystemPolicy",
"elasticfilesystem:DescribeFileSystems",
"elasticfilesystem:DescribeLifecycleConfiguration",
"elasticfilesystem:DescribeMountTargets",
"elasticfilesystem:DescribeMountTargetSecurityGroups",
"elasticfilesystem:DescribeTags"
"elasticfilesystem:ListTagsForResource",
"elasticfilesystem:PutBackupPolicy",
"elasticfilesystem:PutFileSystemPolicy",
"elasticfilesystem:PutLifecycleConfiguration",
"elasticfilesystem:Restore",
"elasticfilesystem:TagResource",
"elasticfilesystem:UntagResource",
"elasticfilesystem:UpdateFileSystem",
"elasticloadbalancing:AddTags",
"elasticloadbalancing:CreateListener",
"elasticloadbalancing:CreateLoadBalancer",
"elasticloadbalancing:CreateTargetGroup",
"elasticloadbalancing:DeleteListener",
"elasticloadbalancing:DeleteLoadBalancer",
"elasticloadbalancing:DeleteTargetGroup",
"elasticloadbalancing:DeregisterTargets",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"elasticloadbalancing:DescribeTargetGroups",
"elasticloadbalancing:DescribeTargetHealth",
"elasticloadbalancing:ModifyTargetGroup",
"elasticloadbalancing:RegisterTargets",
"elasticloadbalancing:RemoveTags",
"elasticloadbalancing:SetSecurityGroups",
"elasticloadbalancing:SetSubnets",
"events:DeleteRule",
"events:DescribeRule",
"events:ListTargetsByRule",
"events:PutRule",
"events:PutTargets",
"events:RemoveTargets",
"iam:AddRoleToInstanceProfile",
"iam:AttachRolePolicy",
"iam:CreateInstanceProfile",
"iam:CreateRole",
"iam:CreateServiceLinkedRole",
"iam:DeleteInstanceProfile",
"iam:DeleteRole",
"iam:DeleteRolePolicy",
"iam:DetachRolePolicy",
"iam:GetContextKeysForPrincipalPolicy",
"iam:GetInstanceProfile",
"iam:GetRole",
"iam:ListAccountAliases",
"iam:ListAttachedRolePolicies",
"iam:ListInstanceProfiles",
"iam:ListInstanceProfilesForRole",
"iam:ListRolePolicies",
"iam:PassRole",
"iam:PutRolePolicy",
"iam:RemoveRoleFromInstanceProfile",
"iam:SimulatePrincipalPolicy",
"kinesis:CreateStream",
"kinesis:DeleteStream",
"kinesis:DescribeStream",
"kinesis:PutRecord",
"kms:CreateGrant",
"kms:Decrypt",
"kms:DescribeKey",
"kms:Encrypt",
"kms:GenerateDataKeyWithoutPlaintext",
"kms:GetKeyPolicy",
"kms:ListAliases",
"kms:ListKeys",
"kms:ReEncryptFrom",
"kms:ReEncryptTo",
"lambda:ListFunctions",
"ram:AssociateResourceShare",
"ram:CreateResourceShare",
"ram:DeleteResourceShare",
"ram:DisassociateResourceShare",
"ram:GetResourceShareAssociations",
"ram:GetResourceShares",
"ram:ListPrincipals",
"ram:ListResources",
"ram:ListResourceSharePermissions",
"ram:TagResource",
"ram:UntagResource",
"rds:AddTagsToResource",
"rds:CopyDBClusterSnapshot",
"rds:CopyDBSnapshot",
"rds:CreateDBClusterSnapshot",
"rds:CreateDBInstance",
"rds:CreateDBSnapshot",
"rds:DeleteDBCluster",
"rds:DeleteDBClusterSnapshot",
"rds:DeleteDBInstance",
"rds:DeleteDBSnapshot",
"rds:DescribeAccountAttributes",
"rds:DescribeDBClusterParameterGroups",
"rds:DescribeDBClusterParameters",
"rds:DescribeDBClusters",
"rds:DescribeDBClusterSnapshots",
"rds:DescribeDBEngineVersions",
"rds:DescribeDBInstances",
"rds:DescribeDBParameterGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeDBInstanceOptions",
"rds:DescribeDBClusterSnapshotAttribute",
"rds:ModifyDBCluster",
"rds:ModifyDBClusterSnapshotAttribute",
"rds:ModifyDBInstance",
"rds:ModifyDBSnapshotAttribute",
"rds:RemoveTagsFromResource",
"rds:RestoreDBClusterFromSnapshot",
"rds:RestoreDBInstanceFromDBSnapshot",
"s3:DeleteObject",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:PutObject",
"s3:_restoreObject",
"servicequotas:ListServiceQuotas",
"sns:CreateTopic",
"sns:DeleteTopic",
"sns:ListSubscriptionsByTopic",
"sns:ListTopics",
"sns:SetTopicAttributes",
"sns:Subscribe",
"sns:Unsubscribe",
"sqs:CreateQueue",
"sqs:SendMessage",
"sqs:SetQueueAttributes",
"ssm:DescribeAssociation",
"ssm:DescribeDocument",
"ssm:DescribeInstanceInformation",
"ssm:GetCommandInvocation",
"ssm:GetDeployablePatchSnapshotForInstance",
"ssm:GetDocument",
"ssm:GetManifest",
"ssm:GetParameter",
"ssm:GetParameters",
"ssm:ListAssociations",
"ssm:ListInstanceAssociations",
"ssm:PutComplianceItems",
"ssm:PutConfigurePackageResult",
"ssm:PutInventory",
"ssm:SendCommand",
"ssm:UpdateAssociationStatus",
"ssm:UpdateInstanceAssociationStatus",
"ssm:UpdateInstanceInformation",
"ssmmessages:CreateControlChannel",
"ssmmessages:CreateDataChannel",
"ssmmessages:OpenControlChannel",
"ssmmessages:OpenDataChannel",
"sts:AssumeRole"}
Considerations and Limitations

When you plan to deploy and configure Veeam Backup for AWS, keep in mind the following limitations and considerations.

**IMPORTANT**

Veeam Backup for AWS is available only in AWS Global and AWS GovCloud (US) regions.

**Licensing**

If the license file is not installed, Veeam Backup for AWS will operate in the *Free* edition allowing you to protect up to 10 instances free of charge.

**Hardware**

The minimum recommended EC2 instance type for the backup appliance is *t3.medium*. For the list of all existing instance types, see [AWS Documentation](https://aws.amazon.com/documentation/ec2/instance-types/).

**Software**

To access Veeam Backup for AWS, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version). Internet Explorer is not supported.

**Security Certificates**

Veeam Backup for AWS supports certificates only in the .PFX and .P12 format.

**Backup Repositories**

Before you start managing backup repositories, consider the following:

- Amazon S3 buckets with the S3 Object Lock enabled are not supported.
- Amazon S3 buckets using server-side encryption with AWS KMS keys (CMK) are not supported.
- Veeam Backup for AWS allows you to store backups only in the S3 Standard, S3 Glacier and S3 Glacier Deep Archive storage classes. The S3 Standard-IA and S3 One Zone-IA storage classes are not supported.
- You cannot change Amazon S3 buckets, folders and storage classes for backup repositories already added to the Veeam Backup for AWS infrastructure.
- When you add a backup repository of the S3 Glacier or S3 Glacier Deep Archive storage class, Veeam Backup for AWS does not create any S3 Glacier vaults in your AWS environment — it assigns the selected storage class to backups stored in the repository. That is why these backups remain in Amazon S3 and cannot be accessed directly through the Amazon S3 Glacier service.
- If you plan to use [AWS Key Management Service (KMS) keys](https://aws.amazon.com/kms/) to encrypt backup repositories, mind that only symmetric KMS keys are supported.
  - If you use a KMS key to encrypt a repository, do not disable or delete this key. Otherwise, Veeam Backup for AWS will not be able to encrypt and decrypt data stored in the repository.
Even though an Amazon S3 bucket is no longer used as a backup repository, Veeam Backup for AWS preserves all backup files previously stored in the repository and keeps these files in Amazon S3.

If you no longer need the backed-up data, either delete it as described in section Managing Backed-Up Data before you remove the repository from the Veeam Backup for AWS infrastructure, or use the AWS Management Console to delete the data if the repository has already been removed.

Backup

Before you start protecting AWS resources, consider the following:

- Veeam Backup for AWS protects only EC2 instances that run in VPCs. EC2-Classic instances are not supported. For more information, see this Veeam KB article.
- When Veeam Backup for AWS backs up EC2 instances with IPv6 addresses assigned, it does not save the addresses. That is why when you restore these instances, IP addresses are assigned according to the settings specified in AWS for the subnet to which the restored instances will be connected.
- Veeam Backup for AWS does not support backup and restore of RDS Multi-AZ DB clusters.
- Snapshot replication is not supported for Aurora multi-master clusters.
- Veeam Backup for AWS supports backup of EFS file systems only to the same AWS accounts where the source file systems belong.
- Indexing of the backed up EFS file systems is not supported in the Free edition of Veeam Backup for AWS. For more information on license editions, see Licensing.
- Veeam Backup for AWS does not support backup of the following VPC configuration components: VPC Traffic Mirroring, AWS Network Firewall, VPC Flow Logs, carrier gateways, customer IP pools, and core networks in route tables.

Restore

Before you start restoring AWS resources, consider the following:

- When restoring multiple EC2 instances that have the same EBS volume attached, Veeam Backup for AWS restores one volume per each instance and enables the Multi-Attach option for every restored volume. For more information on Amazon EBS Multi-Attach, see AWS Documentation.
- Restore of files and folders is supported only for the following file systems: FAT, FAT32, NTFS, ext2, ext3, ext4, XFS, Btrfs.
  For EC2 instances running Microsoft Windows OSes, Veeam Backup for AWS supports file-level restore only for basic volumes.
- When restoring Aurora DB clusters to a new location, Veeam Backup for AWS creates only primary DB instances in the restored clusters. Additional writer DB instances (for Aurora multi-master clusters) or Aurora Replicas (for Aurora DB clusters with single-master replication) must be added manually in the AWS Management Console after the restore operation completes. To learn how to add DB instances to Amazon Aurora DB clusters, see AWS Documentation.
- Veeam Backup for AWS supports restore of EFS file systems only to the same AWS account where the source file systems belong.
- Restore of entire VPC configurations to a new location is not supported for the following VPC configuration items: Client VPN endpoints, customer gateways and load balancer listeners that use authentication certificates and specific components of route tables (core networks, routes to AWS Outpost local gateways, network interfaces, instances and carrier gateways).
• Restore of specific VPC configuration items to a new location is not supported.
Licensing

Veeam Backup for AWS is licensed per protected instance. An instance is defined as a single AWS resource — EC2 instance, RDS resource or EFS file system. An instance is considered to be protected if it has a restore point (snapshot or backup) created by a backup policy during the past 31 days. Each protected instance consumes 1 license unit. However, if an instance has only manually created snapshots or backups, it does not consume any license units.

**NOTE**

If an instance has not been backed up within the past 31 days, Veeam Backup for AWS automatically revokes the license unit from the instance. If you need to manually revoke a license unit, follow the instructions provided in section *Revoking License Units*.

Product Editions

Veeam Backup for AWS is available in 3 editions:

- **Free**
  
  Veeam Backup for AWS operating in the *Free* edition allows you to protect up to 10 instances free of charge. Mind that, this license edition does not support indexing of EFS file systems.

  **TIP**

  If you previously had the *Free* edition installed for evaluation and testing purposes and want to switch to any of the commercial editions without reconfiguring the backup infrastructure, follow the steps described in this Veeam KB article.

- **Paid**

  Veeam Backup for AWS operating in the *Paid* edition allows you to protect an unlimited number of instances.

  In the *Paid* edition of the product, you are charged by the number of instances that you actually protect. To track data protection operations on the backup appliance, Veeam Backup for AWS uses the *AWS Marketplace Metering Service*. Every hour, the backup appliance sends information on the current number of protected instances to AWS. The billing for the protected instances is included into the monthly *AWS Cost and Usage report*.

- **BYOL (Bring Your Own License)**

  Veeam Backup for AWS operating in the *BYOL* edition allows you to use a Veeam Backup for AWS license with a certain number of license units to protect instances.

  For details on how to obtain the license, contact a Veeam sales representative at *Sales Inquiry*. For details on how to install the license on the backup appliance, see *Installing and Removing License*. Note that if the license is not installed, Veeam Backup for AWS operates in the *Free* edition allowing you to protect up to 10 instances free of charge.

**NOTE**

Veeam Backup & Replication licensing is applied to Veeam Backup for AWS appliances managed by standalone Veeam Backup & Replication servers. For more information, see the *Integration with Veeam Backup & Replication Guide*.
Installing and Removing License

This section applies only to the *BYOL* edition of Veeam Backup for AWS.

**IMPORTANT**

If your backup appliance is connected to a standalone Veeam Backup & Replication server, you can manage the license only using the Veeam Backup & Replication console. For more information, see [Integration with Veeam Backup & Replication Guide](#).

### Installing License

To install or update a license installed on the backup appliance, do the following:

1. Switch to the [Configuration](#) page.
2. Navigate to [Licensing > License Info](#).
3. Click [Install License](#).
4. In the [Upload file](#) window, click [Browse](#) to browse to a license file, and then click [Upload](#).

![License Upload Window](image)

### Removing License

To remove a license installed on the backup appliance if you no longer need it:

1. On the [License Info](#) tab, click [Remove License](#).
2. In the **Remove License** window, click **Yes** to confirm that you want to remove the license.

![Image of Veeam Backup for AWS interface]

After you remove the license, Veeam Backup for AWS will automatically switch back to the **Free** edition. In this case, according to the FIFO (first-in first-out) queue, only the first 10 instances registered in the configuration database will remain protected. You can revoke license units from these instances as described in section **Revoking License Units**.

**Related Topics**

Viewing License Information
Viewing License Information

To view details on the license that is currently installed on the backup appliance, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Licensing > License Info**.

The licensing section provides general information on the Veeam Backup for AWS license:

- **Status** — the license status. The status depends on the license edition, the number of days remaining until license expiration and the number of days remaining in the grace period (if any).

- **Instances** — the total number of protected instances that consume license units.

  Each instance that has a restore point created in the past 31 days is considered to be protected and consumes 1 license unit. To view the list of instances that consume license units, switch to the **License Usage** tab.

- **Expiration Date** — the date when the license will expire.

- **License Type** — the license edition (**Free**, **Paid**, **Subscription**).

**NOTE**

*Subscription* is the name of the **BYOL** license in Veeam Backup for AWS.

- **License ID** — the unique identification number of the provided license file (required for contacting the Veeam Customer Support Team).

- **Licensed To** — the name of an organization to which the license was issued.

- **Support ID** — the unique identification number of the support contract (required for contacting the Veeam Customer Support Team).

**Related Topics**

- **Installing and Removing License**
- **Revoking License Units**
Revoking License Units

By default, Veeam Backup for AWS automatically revokes a license unit from a protected instance if no new restore points have been created by the backup policy during the past 31 days. However, you can manually revoke license units from protected instances — this can be helpful, for example, if you remove a number of instances from a backup policy and do not want to protect them anymore.

To revoke a license unit from a protected instance, do the following:

1. Switch to the Configuration page.
2. Navigate to Licensing > License Usage.
3. Select the instance that you no longer want to protect.
4. Click Revoke License.
5. In the Revoke License window, click Yes to confirm that you want to revoke the license unit.
Architecture Overview

The Veeam Backup for AWS infrastructure includes the following components:

- **Backup appliance**
- **Backup repositories**
- **Worker instances**

Backup Appliance

The backup appliance is a Linux-based EC2 instance where Veeam Backup for AWS is installed. The backup appliance performs the following administrative activities:

- Manages infrastructure components.
- Coordinates snapshot creation, backup and recovery tasks.
- Controls backup policy scheduling.
- Generates daily reports and email notifications.

Backup Appliance Components

The backup appliance uses the following components:

- **Backup service** — coordinates data protection and disaster recovery operations.
- **Configuration database** — stores data collected for the Veeam Backup for AWS infrastructure, backup policies, sessions and so on.
- **Web UI** — provides a web interface that allows user to access to the Veeam Backup for AWS functionality.
- **Updater service** — allows Veeam Backup for AWS to check, view and install product and package updates.
- **Self Backup service** — allows Veeam Backup for AWS to backup and restore the configuration database of the backup appliance.
- **REST API service** — allows users to perform operations with Veeam Backup for AWS entities using HTTP requests and standard HTTP methods. For details, see the Veeam Backup for AWS REST API Reference.

Backup Repositories

A backup repository is a folder in an Amazon S3 bucket where Veeam Backup for AWS stores image-level backups of EC2 instances and additional copies of Amazon VPC configurations.

To communicate with a backup repository, Veeam Backup for AWS uses **Veeam Data Mover** — the service that runs on a worker instance and that is responsible for data processing and transfer. When a backup policy addresses the backup repository, the Veeam Data Mover establishes a connection with the repository to enable data transfer. To learn how Veeam Backup for AWS communicates with backup repositories, see Managing Backup Repositories.
IMPORTANT

Backup files are stored in backup repositories in the native Veeam format and must be modified neither manually nor by 3rd party tools. Otherwise, Veeam Backup for AWS may fail to restore the backed-up data.

Encryption on Backup Repositories

For enhanced data security, Veeam Backup for AWS allows you to enable encryption at the repository level. Veeam Backup for AWS encrypts backup files stored in backup repositories the same way as Veeam Backup & Replication encrypts backup files stored in backup repositories. To learn what algorithms Veeam Backup & Replication uses to encrypt backup files, see the Veeam Backup & Replication User Guide, section Encryption Standards. To learn how to enable encryption at the repository level, see Adding Backup Repositories.

Veeam Backup for AWS also supports scenarios where data is backed up to S3 buckets with enabled Amazon S3 default encryption. You can add the S3 bucket to the backup infrastructure as a backup repository and use it as a target for image-level backups. For information on Amazon S3 default encryption, see AWS Documentation.

Worker Instances

A worker instance is a Linux-based EC2 instance that is responsible for the interaction between the backup appliance and other components of the Veeam Backup for AWS infrastructure. Worker instances process backup workload and distribute backup traffic when transferring data to backup repositories.

Veeam Backup for AWS automatically launches a worker instance in Amazon EC2 for the duration of a backup, restore or backup retention process and removes it immediately after the process is complete. Veeam Backup for AWS launches one worker instance per each AWS resource specified in a backup policy, restore or retention task. To minimize cross-region traffic charges, depending on the data protection and disaster recovery operation, Veeam Backup for AWS launches the worker instance in the following location:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Worker Instance Location</th>
<th>Default Worker Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating EC2 image-level backups</td>
<td>AWS Region in which a processed EC2 instance resides</td>
<td>• c5.large — if the total EBS volume size is less than 1024 GB</td>
</tr>
<tr>
<td>EC2 instance restore</td>
<td>AWS Region to which an EC2 instance is restored</td>
<td>• c5.xlarge — if the total EBS volume size is 1024-1250 GB</td>
</tr>
<tr>
<td>EC2 volume-level restore</td>
<td>AWS Region to which the volumes of a processed EC2 instance are restored</td>
<td>• c5.2xlarge — if the total EBS volume size is more than 1250 GB</td>
</tr>
<tr>
<td>Performing health check for EC2 backups</td>
<td>AWS Region in which a backup repository with backed-up data resides</td>
<td></td>
</tr>
<tr>
<td>Creating EC2 archived backups</td>
<td>AWS Region in which a standard backup repository with backed-up data resides</td>
<td>• c5.2xlarge</td>
</tr>
<tr>
<td>EC2 file-level restore from cloud-native snapshots or replicated snapshots</td>
<td>AWS Region in which a snapshot is located</td>
<td>• t3.medium</td>
</tr>
</tbody>
</table>
Worker Instance Components

A worker instance uses the following components:

- **Veeam Data Mover** — the service that performs data processing tasks. During backup, the Veeam Data Mover retrieves EC2 instance data from snapshots and stores the retrieved data to backup repositories. During restore, the Veeam Data Mover transfers backed-up data from backup repositories to the target location.

- **File-level recovery browser** — the web service that allows you to find and save files and folders of a backed-up EC2 instance to the local machine. The file-level recovery browser is installed automatically on every worker instance that is launched for file-level recovery.

Security Certificates for Worker Instances

Veeam Backup for AWS uses self-signed TLS certificates to establish secure communication between the web browser on the local machine and the file-level recovery browser on the worker instance during file-level restore. A self-signed certificate is generated automatically on the worker instance when the restore session starts.
Deployment

Veeam Backup for AWS comes as an image of a Linux-based EC2 instance that you can deploy using one of the following installation options:

- **Installing Veeam Backup for AWS from AWS Marketplace** (recommended) — allows you to use a CloudFormation template to deploy Veeam Backup for AWS with most of the backup appliance settings configured out of the box.

- **Launching Veeam Backup for AWS from an Amazon Machine Image (AMI)** — allows you to deploy Veeam Backup for AWS from an AMI and to configure the backup appliance settings manually.
Installing Veeam Backup for AWS from AWS Marketplace

Veeam Backup for AWS is installed on a single EC2 instance. The EC2 instance is created during the product installation.

To install Veeam Backup for AWS from AWS Marketplace:

1. Log in to AWS Marketplace using credentials of an AWS account in which you plan to install Veeam Backup for AWS.

   You can install Veeam Backup for AWS in the production site — in the AWS account where resources that you plan to back up reside. It is recommended, however, that you use a separate AWS account for Veeam Backup for AWS installation. In this case, if a disaster strikes in the production site, you will still be able to access Veeam Backup for AWS and perform recovery operations.

2. Open the Veeam Backup for AWS overview page for the necessary product edition:
   - Veeam Backup for AWS Free Edition
   - Veeam Backup for AWS Paid Edition
   - Veeam Backup for AWS BYOL Edition

For more information on product editions, see Licensing.

3. Click Continue to Subscribe.
4. On the **Subscribe to this software** page, read the product license agreement and click **Continue to Configuration**.

To view the license agreement, expand the details in the **Terms and Conditions** section and click **End User License Agreement**.

5. On the **Configure this software** page, configure installation settings:
   
   a. From the **Delivery Method** drop-down list, choose whether you want to connect the EC2 instance running Veeam Backup for AWS to an existing Amazon VPC and subnet, or to create a new Amazon VPC and subnet for the instance.
      
      - **VB for AWS Deployment - Existing VPC** — select this option if you want to use an existing Amazon VPC and subnet.
      - **VB for AWS Deployment - New VPC** — select this option if you want to create a new Amazon VPC and subnet.

      For more information on Amazon VPCs and subnets, see [AWS Documentation](https://aws.amazon.com/documentation/).

   b. From the **Software Version** drop-down list, select the latest version of Veeam Backup for AWS.

   c. From the **Region** drop-down list, select an AWS Region in which the EC2 instance running Veeam Backup for AWS will reside.

      For more information on AWS Regions, see [AWS Documentation](https://aws.amazon.com/documentation/).
6. Click **Continue to Launch**.

7. On the **Launch this software** page, do the following:
   
   a. In the **Configuration Details** section, review the product installation settings.
   
   b. From the **Choose Action** drop-down list, select **Launch CloudFormation**.
   
   c. Click **Launch**. The Create stack wizard will open.

   Veeam Backup for AWS is installed using AWS CloudFormation stacks. In AWS CloudFormation, a stack is a collection of AWS services and resources that you can manage as a single unit. You can create a stack in an AWS account, use resources included in the stack to run an application, or delete a stack if you no longer need it. For more information on AWS CloudFormation stacks, see [AWS Documentation](https://aws.amazon.com/documentation/cloudformation). In the Create stack wizard, you will create a stack for Veeam Backup for AWS.
8. At the **Specify template** step of the wizard, the stack template settings are preconfigured by Veeam Backup for AWS and cannot be changed.

9. At the **Specify stack details** step of the wizard, configure the following stack settings:
   
a. In the **Stack name** field, specify a name for the new stack.

   **Stack name**

   Stack name

   dept-01-vbaws-srv

   Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

   b. In the **Instance Configuration** section, do the following:

   i. Select the EC2 instance type for the backup appliance.

      The recommended EC2 instance type is **t3.medium**.
ii. Select a key pair that will be used to authenticate against the backup appliance.

For a key pair to be displayed in the Key pair for Veeam Backup for AWS server list, it must be created in the Amazon EC2 console. To learn how to create key pairs, see AWS Documentation.

![Instance Configuration]

<table>
<thead>
<tr>
<th>Instance Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance type for Veeam Backup for AWS server</td>
</tr>
<tr>
<td>t2.medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key pair for Veeam Backup for AWS server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select one, or create a new one at AWS console</td>
</tr>
<tr>
<td>dev_lab</td>
</tr>
</tbody>
</table>

c. In the **Network Configuration** section, do the following:

i. Select *true* if you want to create an Elastic IP address for the backup appliance.

For more information on Elastic IP addresses, see AWS Documentation.

ii. Specify the IPv4 address ranges from which Veeam Backup for AWS Web UI will be accessible.

Make sure the IPv4 address of the local machine from which you plan to access Veeam Backup for AWS lies within the specified IPv4 range.

The IPv4 address ranges must be specified in the CIDR notation (for example, 12.23.34.0/24). To let all IPv4 addresses access Veeam Backup for AWS, you can specify 0.0.0.0/0. Note that allowing access from all IPv4 addresses is unsafe and thus not recommended in production environments.

Based on the specified IPv4 ranges, AWS CloudFormation will create a security group for Veeam Backup for AWS with an inbound rule for HTTPS traffic. By default, port 443 is open for the inbound HTTPS traffic. If you plan to change the security group for Veeam Backup for AWS upon the product installation, you will need to manually add inbound rules to the new security group and make sure this security group allows access to AWS services listed in the AWS Services section.

![Network Configuration]

<table>
<thead>
<tr>
<th>Network Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create elastic IP for Veeam Backup for AWS server?</td>
</tr>
<tr>
<td>By default a dynamic IP will be created (and it could change during reboots of this instance)</td>
</tr>
<tr>
<td>true</td>
</tr>
</tbody>
</table>

| Allowed source IP addresses for connection to HTTPS |
| The IP address range in CIDR format (e.g. 12.23.34.0/24) from which Veeam Backup for AWS Management portal will be accessible |
| 12.23.34.0/24 |

d. In the **VPC and Subnet** section, specify an Amazon VPC and subnet to which the backup appliance will be connected.

Depending on the option selected at step 5a, you can either select an existing Amazon VPC and subnet, or specify IPv4 address ranges in the CIDR notation for the new Amazon VPC and subnet.
IMPORTANT
Consider the following:

- The specified Amazon VPC and subnet must have the outbound internet access to AWS services listed in the **AWS Services** section.
- The specified Amazon VPC and subnet must allow the inbound internet access from the local machine from which you plan to access Veeam Backup for AWS.

To learn how to enable internet access for Amazon VPCs and subnets, see **AWS Documentation**.

10. At the **Configure stack options** step of the wizard, specify AWS tags, IAM role permissions and other additional settings for the stack.

For more information on available stack options, see **AWS Documentation**.

11. At the **Review** step of the wizard, do the following:

   a. Review the configured settings.

   b. Select the **I acknowledge that AWS CloudFormation might create IAM resources** check box.
c. Click **Create stack**.

Right after installation, you must accept license agreements and create a default user. To learn how to do that, see **After You Install**.
After You Install

After you install Veeam Backup for AWS, you must perform the following steps to start working on the backup appliance:

1. In a web browser, navigate to the Veeam Backup for AWS web address.
   
   The address consists of a public IPv4 address or DNS hostname of the backup appliance and is available over HTTPS only. For more information, see Accessing Veeam Backup for AWS.

   **IMPORTANT**

   Internet Explorer is not supported. To access Veeam Backup for AWS, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version).

2. Read and accept the Veeam license agreement, Veeam licensing policy, 3rd party components and software license agreements. If you reject the agreements, you will not be able to continue installation.

3. In the **Instance ID** field, specify the AWS ID of the EC2 instance running Veeam Backup for AWS to prove that you are the owner of this EC2 instance.
   
   You can find the EC2 instance AWS ID in the AWS Management Console.

4. Create a default user whose credentials you will use for your first login to Veeam Backup for AWS. A user name cannot be admin, can contain only lowercase Latin letters, numeric characters, underscores and dashes. You can use the dollar sign ($) as the last character of the name. The maximum length of the name is 32 characters.
   
   Veeam Backup for AWS will create the default user and display the welcome screen where you can log in.

   **NOTE**

   To increase the security of the default user account, it is recommended that you enable multi-factor authentication (MFA) for the account after you first log in to Veeam Backup for AWS. To learn how to enable MFA, see Configuring Multi-Factor Authentication.
Installing Veeam Backup for AWS from AMI

Veeam Backup for AWS is installed on a single EC2 instance. The EC2 instance is created during the product installation.

**IMPORTANT**

After you install Veeam Backup for AWS from the Amazon Machine Image (AMI), you will be asked to provide one-time access keys of an IAM user that Veeam Backup for AWS will use to create IAM roles required for the backup appliance configuration. If you do not want to provide the keys, you can create the required IAM roles manually before you begin the installation. For more information on the required IAM roles, see Required IAM Permissions.

To install Veeam Backup for AWS from the AMI:

1. Log in to the AWS Management Console using credentials of an AWS account in which you plan to install Veeam Backup for AWS.
   
   You can install Veeam Backup for AWS in the production site — in the AWS account where resources that you plan to back up reside. It is recommended, however, that you use a separate AWS account for Veeam Backup for AWS installation. In this case, if a disaster strikes in the production site, you will still be able to access Veeam Backup for AWS and perform recovery operations.

2. Use the region selector in the upper-right corner of the page to select an AWS Region in which the EC2 instance running Veeam Backup for AWS will reside.
   
   For more information on AWS Regions, see AWS Documentation.

3. In the AWS services section, expand the All services menu and navigate to Compute > EC2.

4. On the EC2 Dashboard tab, click Launch instance > Launch instance. The launch instance wizard will open.
5. At the Choose an Amazon Machine Image (AMI) step of the wizard, open the Community AMIs tab. Then, in the search field, type veeam-aws and press [ENTER] on the keyboard.

Choose the necessary product edition (Free, Paid or BYOL) and click Select. For more information on product editions, see Licensing.

6. At the Choose an Instance Type step of the wizard, select an EC2 instance type for the backup appliance. The minimum recommended EC2 instance type is t3.medium.
7. At the **Configure Instance Details** of the wizard, do the following:

   a. In the **Network** and **Subnet** fields, specify an Amazon VPC and subnet to which the backup appliance will be connected. You can either select an existing Amazon VPC and subnet, or create a new Amazon VPC and subnet.

   For more information on Amazon VPCs and subnets, see **AWS Documentation**.

   **IMPORTANT**

   Consider the following:

   - The specified Amazon VPC and subnet must have the outbound internet access to AWS services listed in the **AWS Services** section.
   - The specified Amazon VPC and subnet must allow the inbound internet access from the local machine that you plan to use to access Veeam Backup for AWS.

   To learn how to enable internet access for Amazon VPCs and subnets, see **AWS Documentation**.

   b. From the **Auto-assign Public IP** drop-down list, select **Enable**.

   c. [Applies if you have created IAM roles required for the product installation beforehand] In the **IAM role** field, specify the **Impersonation** IAM role that will be attached to the backup appliance. This role will allow Veeam Backup for AWS to assume IAM roles to perform backup and restore operations.

   d. In the **Advance Details** section, enable access to the instance metadata to allow Veeam Backup for AWS to use the Instance Metadata Service (IMDS) to be able to configure and manage the running backup appliance. To do that, select **Enabled** from the **Metadata accessible** drop-down list.

   e. Configure additional settings for the backup appliance to meet your organization requirements. To learn how to configure Amazon Linux instances, see **AWS Documentation**.
8. **At the Add Storage** step of the wizard, review the preconfigured storage settings and click **Next: Add Tags**. For technical reasons, it is not recommended to change these settings.

9. **At the Add Tags** step of the wizard, you can specify AWS tags that will be assigned to the backup appliance. For example, you can specify a name that will help you easily identify and locate the appliance.

10. **At the Configure Security Group** step of the wizard, choose a security group that will control the inbound and outbound traffic for the backup appliance. You can either associate an existing security group with the backup appliance or create a new security group.

   - If you choose an existing security group, make sure it allows access to AWS services listed in the **AWS Services** section.
   
   - If you choose to create a new security group, add a new inbound rule for the HTTPS traffic:
     
     i. Click **Add Rule**.
     
     ii. Select **HTTPS** from the **Type** drop-down list and enter 443 in the **Port Range** field.
     
     iii. In the **Source** column, specify IPv4 address ranges from which Veeam Backup for AWS Web UI will be accessible.

     Make sure the IPv4 address of the local machine from which you plan to access Veeam Backup for AWS lies within the specified IPv4 ranges.
IPv4 address ranges must be specified in the CIDR notation (for example, 12.23.34.0/24). To allow unrestricted access to the backup appliance, you can specify 0.0.0.0/0. However, the latter is not recommended since unrestricted access to Veeam Backup for AWS can violate your organization security policy.

11. At the Review step of the wizard, review the configured settings and click Launch.

Right after installation, you must perform a number of additional actions for the backup appliance configuration. For more information, see After You Install.
Required IAM Permissions

When you install the solution from AWS Marketplace, Veeam Backup for AWS creates 2 IAM roles:

- **Impersonation IAM role** — is attached to the backup appliance and is then used to assume other IAM roles added to the Veeam Backup for AWS infrastructure.

- **Default Backup Restore IAM role** — is automatically added to Veeam Backup for AWS and is assigned all the permissions required to perform operations within the initial AWS account. For example, the role is used to back up AWS resources within the account, to store backups in any Amazon S3 bucket within the account, and so on.

When you install the solution from the AMI, you can either create these IAM roles manually, or instruct Veeam Backup for AWS to use one-time access keys for automatic creation of the required IAM roles.

Creating IAM Roles Manually

If you choose to create IAM roles manually, you must do this in the AWS Management Console before you start installing Veeam Backup for AWS. To learn how to create IAM roles, see Appendix A. Creating IAM Roles in AWS.

The created IAM roles must have specific permissions:

- The **Impersonation IAM role** attached to the backup appliance operating in the **BYOL or Free** license edition must have the following permissions:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "sts:AssumeRole"
         ],
         "Resource": "*"
      }
   ]
}
```
• The *Impersonation* IAM role attached to the backup appliance operating in the *Paid* license edition must have the following permissions:

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Action": [
         "aws-marketplace:MeterUsage"
      ],
      "Resource": "*",
      "Effect": "Allow"
   }
   ]
}
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Action": [
         "sts:AssumeRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
   }
   ]
}
```

• The *Default Backup Restore* IAM role must meet the following requirements:
  o You must allow the *Impersonation* IAM role to assume the *Default Backup Restore* IAM role. To do that, configure trusted relationships for the *Default Backup Restore* IAM role as described in section Appendix A. Creating IAM Roles in AWS.
  o The *Default Backup Restore* IAM role must have permissions required to perform all operations available in Veeam Backup for AWS within the initial AWS account. For more information on the required permissions, see Full List of IAM Permissions.

However, if you plan to use this role for specific operations or do not plan to use this role at all, you can assign the role granular permissions. For more information, see IAM Permissions.

**TIP**
You will be able to add other IAM roles later, after Veeam Backup for AWS installation. For more information, see Managing IAM Roles.

### Using One-Time Access Keys

If you choose to use one-time keys of an IAM user to create IAM roles automatically, no additional steps are required before or during Veeam Backup for AWS installation. However, after installation, you must instruct Veeam Backup for AWS to automatically create IAM roles required for the backup appliance configuration. To learn how to do that, see After You Install.
The IAM user must have the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetRole",
                "ec2:DescribeInstances",
                "iam:GetInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "cloudwatch:DeleteAlarms",
                "ec2:CreateTags",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:AddRoleToInstanceProfile",
                "dlm:CreateLifecyclePolicy",
                "cloudwatch:PutMetricAlarm",
                "iam:PassRole",
                "iam:DetachRolePolicy",
                "iam:SimulatePrincipalPolicy",
                "ec2:DisassociateIamInstanceProfile",
                "iam:DeleteRolePolicy",
                "dlm:DeleteLifecyclePolicy",
                "ec2:AssociateIamInstanceProfile"
            ],
            "Resource": "*"
        }
    ]
}
```
After You Install

To start working with Veeam Backup for AWS, you must perform the initial configuration of the backup appliance. To do that, in a web browser, navigate to the Veeam Backup for AWS web address. The address consists of a public IPv4 address or DNS hostname of the backup appliance and is available over HTTPS only. For more information, see Accessing Veeam Backup for AWS.

**IMPORTANT**

Internet Explorer is not supported. To access Veeam Backup for AWS, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version).

To configure backup appliance settings, complete the Initial Configuration wizard:

1. Read and accept license agreements.
2. Choose a configuration mode.
3. Specify an IAM identity.
4. Create the default user.
5. Install a Veeam Backup for AWS license.
6. Specify a time zone.
7. Finish working with the wizard.
Step 1. Accept License Agreement

At the **License Agreement** step of the wizard, read and accept the Veeam license agreement, Veeam licensing policy, 3rd party components and software license agreements. If you reject the agreements, you will not be able to continue installation.
Step 2. Choose Configuration Mode

At the **Configuration Mode** step of the wizard, choose whether you want to instruct Veeam Backup for AWS to automatically create IAM roles required for the backup appliance configuration, or you want to specify an IAM role created manually.

**IMPORTANT**

If you select the *Manual* configuration mode, make sure you have created the required IAM role beforehand as described in section *Required IAM Permissions*.

<table>
<thead>
<tr>
<th>Initial Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose configuration mode</strong></td>
</tr>
<tr>
<td><strong>Automatic (recommended)</strong></td>
</tr>
<tr>
<td>Set up the appliance by providing temporary access keys. With this option selected, Veeam Backup for AWS will automatically create required IAM roles and a lifecycle policy used to protect the appliance data.</td>
</tr>
<tr>
<td><strong>Manual</strong></td>
</tr>
<tr>
<td>Set up the appliance by providing an IAM role. With this option selected, you must manually create the required IAM roles beforehand as described in the User Guide.</td>
</tr>
</tbody>
</table>
Step 3. Specify IAM Identity

At the **Account** step of the wizard, do the following:

- If you have selected the **Automatic** option at the **Configuration Mode** step of the wizard, specify one-time access keys that will be used to create the Impersonation and Default Backup Restore IAM roles. For more information on the IAM roles, see [Required IAM Permissions](#).

- If you have selected the **Manual** option at the **Configuration Mode** step of the wizard, specify the Default Backup Restore IAM role that will be added to the Veeam Backup for AWS and used to perform operations.

### Specifying One-Time Access Keys

To specify the access key ID and the secret access key of an IAM user, use the **Access key** and **Secret key** fields. Note that the IAM user must be authorized to create IAM roles. To learn what permissions the IAM user must have to create IAM roles, see [Required IAM Permissions](#).

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.

### Specifying IAM Role

To specify the **Default Backup Restore** IAM role, enter the IAM role name specified in AWS when creating the role. The IAM role must be created beforehand as described in [Required IAM Permissions](#).

**NOTE**

If there is a path identifying the IAM role, you must specify the role name in the **PATH/NAME** format (for example, `dept_1/s3_role`). To learn how to add identifiers to IAM roles, see [AWS Documentation](#).

You can check whether the specified IAM role has permissions required to perform all Veeam Backup for AWS operations. To run the IAM role permission check, click **Check Permissions**. If the IAM role permissions are insufficient, Veeam Backup for AWS will display a warning, but you will still be able to proceed with the wizard without granting the missing permissions to the role. To learn how to grant permissions to IAM roles using the AWS Management Console, see [AWS Documentation](#).
**TIP**

You can grant permissions to this IAM role and add other IAM roles that will be used to perform backup and restore operations later, after the backup appliance configuration completes. For more information, see Managing IAM Roles.

---

**Veeam Backup for AWS**

**Initial Configuration**

<table>
<thead>
<tr>
<th>License Agreement</th>
<th>Configuration Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Account**

- **IAM role**: oz-v6-default-role

**Required Permissions**

Veeam Backup for AWS automatically creates a JSON file with the list of all required permissions. Add the permissions to an IAM policy attached to the specified IAM role and run the permission check again.

**Download**

---
Step 4. Create Default User

At the **Default User** step of the wizard, create the default user whose credentials you will use for your first login to Veeam Backup for AWS.

Mind that the specified user name cannot be *admin*, can contain only lowercase Latin letters, numeric characters, underscores and dashes. You can use the dollar sign ($) as the last character of the name. The maximum length of the name is 32 characters.

**NOTE**

To increase the security of the default user, it is recommended that you enable multi-factor authentication (MFA) for the user account after you first log in to Veeam Backup for AWS. To learn how to enable MFA, see [Configuring Multi-Factor Authentication](#).

![Veeam Backup for AWS Configuration](#)

**Specify credentials for default user**

Enter a name and password for the default administrator account that will be used to access the Veeam Backup for AWS web UI.

- **Name**: *administrator*
- **Password**: **********
  
  Password must be 8 characters minimum with one digit, one uppercase and one lowercase. Non-alphabetic sequences such as 1234 are not allowed.

  Re-enter password: **********
Step 5. Install License

At the License step of the wizard, browse to the license file supplied to you by Veeam. You will still be able to proceed with the wizard without providing a license — in this case, the Free edition of Veeam Backup for AWS will be installed.

**TIP**
You can install a valid license later, after the backup appliance configuration completes. For more information, see Installing and Removing License.
Step 6. Specify Time Zone

Since the backup appliance is deployed on an EC2 instance in Amazon EC2, the time zone is set to Coordinated Universal Time (UTC) by default. However, you can change the time zone at the Time Zone step of the wizard if required. For example, you may want the time on the backup appliance to match the time on the local machine from which you access Veeam Backup for AWS.

TIP

You can change time zone settings later, after the backup appliance configuration completes. For more information, see Changing Time Zone.
Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration settings and click **Finish**. After the initial configuration process completes, Veeam Backup for AWS will display the welcome screen where you can log in.

---

**Initial Configuration**

| License Agreement | Review configured settings
| --- | --- |
| Configuration Mode | Review the settings, and click **Apply** to start the appliance configuration.
| Account |  |
| Default User |  |
| License |  |
| Time Zone |  |
| Summary |  |

![Configuration Screen](image)

---

**License Agreement**

**Configuration Mode**

**Account**

**Default User**

**License**

**Time Zone**

**Summary**

**Review configured settings**

- **Copy to Clipboard**

**General settings**

- License type: **RIO**
- Time Zone: **Europe/Prague +01:00**

**Account information**

- Default administrator account: **administrator**
Uninstalling Veeam Backup for AWS

Depending on the installation option you chose to deploy Veeam Backup for AWS, use one of the following options to uninstall the solution:

- If you deployed a backup appliance from AWS Marketplace, you must delete the CloudFormation stack created while installing Veeam Backup for AWS. All resources included in the stack will be deleted automatically.
- If you deployed a backup appliance from the AMI, you must manually delete AWS resources created while installing Veeam Backup for AWS.

**IMPORTANT**
When you deploy Veeam Backup for AWS from the Veeam Backup & Replication console, the CloudFormation stack is not created and AWS resources cannot be managed as a single unit. Keep in mind that these resources are not automatically deleted from AWS when you remove the backup appliance from the Veeam Backup & Replication infrastructure. To learn how to manually delete resources created during Veeam Backup for AWS installation, see the Integration with Veeam Backup for AWS Guide, section Removing Appliances.

Note that backed-up data will not be removed automatically after you uninstall the solution. You can keep this data in your AWS environment and import it to a new backup appliance:

- To import cloud-native snapshots, rescan AWS Regions where the snapshots are stored. The snapshots will be automatically imported to the configuration database.
- To import image-level backups, assign the Amazon S3 bucket where the backups are stored to a new backup repository as described in section Adding Backup Repositories.

If you do not want to keep the backed-up data, remove it manually as described in section Managing Backed-Up Data. Alternatively, you can remove the data using the AWS Management Console:

1. Log in to the AWS Management Console using credentials of an AWS account where the data is stored.
2. Use the region selector in the upper-right corner of the page to select the AWS Region in which the backed-up data is stored.
3. Remove the backed-up data:
   - To remove backups, navigate to Services > S3. Select an Amazon S3 bucket where the backups are stored. Navigate to Veeam > Backup, select the backup repository folder, and click Delete.
   - To remove RDS cloud-native snapshots, navigate to Services > RDS > Snapshots, select the necessary Veeam snapshots, and click Delete.
   - To remove EC2 cloud-native snapshots, navigate to Services > EC2 > Snapshots, select the necessary Veeam snapshots, and click Delete.
Deleting CloudFormation Stack

When you deploy a backup appliance from AWS Marketplace, Veeam Backup for AWS is installed using an AWS CloudFormation stack. In AWS CloudFormation, a stack is a collection of AWS services and resources that you can manage as a single unit. To uninstall Veeam Backup for AWS, you must delete the CloudFormation stack from your AWS infrastructure. For more information on working with stacks, see AWS Documentation.

To delete the Veeam Backup for AWS CloudFormation stack, perform the following steps:

1. Log in to the AWS Management Console using credentials of an AWS account where Veeam Backup for AWS is installed.
2. Use the region selector in the upper-right corner of the page to select the AWS Region in which the backup appliance resides.
3. Navigate to Services > CloudFormation.
4. From the Stacks list, select the CloudFormation stack created while installing Veeam Backup for AWS.
5. Click Delete.
6. In the confirmation window, click Delete stack to acknowledge deletion.

**NOTE**

After you acknowledge the operation, the Veeam Backup for AWS CloudFormation stack will acquire the DELETE_IN_PROGRESS state. When all AWS resources included in the stack are successfully deleted, the stack will acquire the DELETE_COMPLETE state. By default, deleted CloudFormation stacks are not displayed in the AWS Management Console. To learn how to view deleted stacks and to troubleshoot deletion issues, see AWS Documentation.
Deleting AWS Resources

When you deploy a backup appliance from the Amazon Machine Image (AMI), Veeam Backup for AWS creates a number of resources while operating in AWS infrastructure, and these resources are not removed from the infrastructure automatically when you delete the backup appliance. To uninstall Veeam Backup for AWS, you must locate and delete the following resources from your AWS infrastructure:

- AWS::IAM::InstanceProfile
- AWS::DLM::LifecyclePolicy
- AWS::CloudWatch::Alarm
- AWS::EC2::SecurityGroup
- AWS::IAM::Role
- AWS::EC2::Instance

To delete a resource, do the following:

1. Log in to the AWS Management Console using credentials of an AWS account where Veeam Backup for AWS is installed.
2. Use the region selector in the upper-right corner of the page to select the AWS Region in which the backup appliance resides.
3. Navigate to AWS service to which the AWS resource belong.
4. Select the AWS resource that you want to remove, and click Delete.
Accessing Veeam Backup for AWS

To access Veeam Backup for AWS, in a web browser, navigate to the Veeam Backup for AWS web address. The address consists of a public IPv4 address or DNS hostname of the backup appliance. Note that the website is available over HTTPS only.

**IMPORTANT**

Internet Explorer is not supported. To access Veeam Backup for AWS, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version).

You can access Veeam Backup for AWS using a local user account or a user account of an external identity provider. To learn how to add user accounts to Veeam Backup for AWS, see [Adding User Accounts](#).

**NOTE**

The web browser may display a warning notifying that the connection is untrusted. To eliminate the warning, you can replace the TLS certificate that is currently used to secure traffic between the browser and the backup appliance with a trusted TLS certificate. To learn how to replace certificates, see [Replacing Security Certificates](#).

Logging In Using Local User Account

To log in using credentials of a Veeam Backup for AWS user account, do the following:

1. In the **Username** and **Password** fields, specify credentials of the user account.
   
   If you log in for the first time, use credentials of the default user that was created after the product installation. In future, you can add other user accounts to grant access to Veeam Backup for AWS. For more information, see [Managing Permissions](#).

   **TIP**

   If you do not remember the user password, you can reset it. To do that, click the **Forgot password?** link and follow the instructions provided in this Veeam KB article.

2. Select the **Remain logged in** check box to save the specified credentials in a persistent browser cookie so that you do not have to provide credentials every time you access Veeam Backup for AWS in a new browser session.
3. Click **Log in**.

If **multi-factor authentication (MFA) is enabled** for the user, Veeam Backup for AWS will prompt you to enter a code to verify the user identity. In the **Verification code** field, enter the temporary six-digit code generated by the authentication application running on your trusted device. Then, click **Log in**.

Logging In Using Identity Provider User Account

**IMPORTANT**

To access Veeam Backup for AWS under a user account of your identity provider, you must first **configure single sign-on settings** and then **add the identity provider user account** to Veeam Backup for AWS.

To log in using an identity provider, do the following:

1. Click **Log in with Single Sign-On**. You will be redirected to your identity provider portal.

2. If you have not logged in yet, log in to the identity provider portal. After that, you will be redirected to the **Veeam Backup for AWS Overview** page as an authorized user.
Logging Out

To log out, at the top right corner of the Veeam Backup for AWS window, click the user name and then click Log out.
Configuring Veeam Backup for AWS

To start working with Veeam Backup for AWS, perform a number of steps for its configuration:

1. **Add IAM roles to access AWS services and resources.**
2. **Add user accounts to control access to Veeam Backup for AWS.**
3. **Configure backup repositories.**
   This step applies if you plan to protect EC2 instances with image-level backups, to perform EFS indexing operations, to back up Veeam Backup for AWS configuration and to keep additional copies of Amazon VPC configuration backups in Amazon S3.
4. **Configure worker instance settings.**
   If you do not configure settings for worker instances, Veeam Backup for AWS will use the default settings of AWS Regions where worker instances will be launched.
5. **Configure global retention, email notification and single-sign-on settings.**

**NOTE**

Even after you add IAM roles that manage your AWS resources and configure all the necessary settings, Veeam Backup for AWS will not populate the list of resources on the Resources page — unless you create backup policies and specify regions where the AWS resources belong, as described in section Performing Backup.
Managing IAM Roles

**NOTE**
This section assumes that you have a good understanding of IAM Roles, Creating IAM Policies and Adding and Removing IAM Identity Permissions.

Veeam Backup for AWS uses permissions of IAM roles to access AWS services and resources, and to perform the backup and restore operations. For example, Veeam Backup for AWS requires access to the following AWS resources:

- **EC2 resources** — to display the list of EC2 instances in backup policy settings, to create cloud-native snapshots, snapshot replicas, to launch worker instances and to restore backed-up data.

- **S3 resources** — to store backed-up data in backup repositories, to perform transform operations with backup chains, and to copy backed-up data from backup repositories to worker instances during restore.

For each data protection and disaster recovery operation performed by Veeam Backup for AWS, you must specify an IAM role:

- If you plan to protect data within the initial AWS account, you can specify the Default Backup Restore IAM role that has been added to Veeam Backup for AWS upon the product installation either from AWS Marketplace or from the AMI using the Automatic configuration mode. This IAM role has already been assigned all the required permissions to perform operations in Veeam Backup for AWS. For more information on the Default Backup Restore IAM role permissions, see Full List of IAM Permissions.

  However, you can also specify a custom IAM role that has granular permissions to perform specific operations within the initial AWS account. For more information on the granular permissions, see IAM Permissions.

- If you plan to protect data of another AWS account, to keep backed-up data in another AWS account, or if you have installed Veeam Backup for AWS from the AMI using the Manual configuration mode, you must specify a custom IAM role that has granular permissions to perform operations in a specific AWS account.

To be able to use a custom IAM role to perform backup and restore operations, you must first add this IAM role to Veeam Backup for AWS. You can add IAM roles that already exist in your AWS accounts, or instruct Veeam Backup for AWS to create and add IAM roles with predefined permission sets. To learn how to add IAM roles in Veeam Backup for AWS, see Adding IAM Roles. To learn how to create IAM roles in the AWS Management Console, see Appendix A. Creating IAM Roles in AWS.
Adding IAM Roles

To add an IAM role to Veeam Backup for AWS, complete the following steps:

1. Launch the Add IAM Role wizard.
2. Specify a name and description for the IAM role.
4. Finish working with the wizard.
Step 1. Launch Add Account Wizard

To launch the Add IAM Role wizard, do the following:

1. Switch to the Configuration page.
2. Navigate to Accounts > IAM Roles.
3. Click Add.
Step 2. Specify IAM Role Name and Description

At the **Role Name** step of the wizard, specify a name and description for the IAM role. The specified name and description will be displayed on the **IAM Roles** tab of the **Accounts** page.

Consider the following limitations:

- The specified name must be unique in Veeam Backup for AWS.
- The length of the name must not exceed 32 characters.
- The length of the specified description must not exceed 255 characters.
Step 3. Specify IAM Role Type and Settings

At the **Role Settings** step of the wizard, choose whether you want to add an already existing IAM role, or to create a new IAM role and add it to Veeam Backup for AWS.

- **IAM role from current account** — select this option if you want to add an IAM role that has permissions to access resources in the initial AWS account.

- **IAM role from another account** — select this option if you want to add a cross-account IAM role that has permissions to access resources in another AWS account.
  
  The cross-account IAM role will be used to provide IAM users in the initial AWS account (the trusted account) access to resources in another AWS account (the trusting account). To learn how to delegate access across AWS accounts using IAM roles, see **AWS Documentation**.

- **Create new IAM role** — select this option if you want to create a new IAM role and add it to Veeam Backup for AWS.

Then, specify the following IAM role settings:

- Specifying settings for an IAM role from the initial AWS account.
- Specifying settings for a cross-account IAM from another account.
- Specifying settings for a new IAM role.

### Specifying Settings for IAM Role

[This step applies if you have selected the **IAM role from current account** option]

At the **Role Settings** step of the wizard, use the **AWS role name** field to enter the IAM role name as specified in AWS.

**NOTE**

If there is a path identifying the IAM role, you must specify the role name in the **PATH/NAME** format (for example, `dept_1/s3_role`). To learn how to add identifiers to IAM roles, see **AWS Documentation**.

### Specifying Settings for Cross-Account IAM Role

[This step applies if you have selected the **IAM role from another account** option]
At the **Role Settings** step of the wizard, specify the following settings:

1. **In the Account ID field**, specify the 12-digit number (or alias) of the trusting account.
   
   The trusting account is an AWS account that owns AWS services and resources, and shares them with the initial AWS account (trusted account). To learn how to delegate access across AWS accounts, see [AWS Documentation](#).

2. **In the AWS role name field**, enter the cross-account IAM role name as specified in AWS.
   
   The cross-account IAM role must be created in the trusting account beforehand, and must allow the trusting account to share AWS services and resources with the trusted account — an AWS account where the backup appliance belongs. To learn how to create cross-account IAM roles, see [AWS Documentation](#).

   **NOTE**

   If there is a path identifying the IAM role, you must specify the role name in the `PATH/NAME` format (for example, `dept_1/s3_role`). To learn how to add identifiers to IAM roles, see [AWS Documentation](#).

3. **In the External ID field**, specify an external ID of the cross-account IAM role.
   
   The external ID is a property in the trust policy of the cross-account IAM role used for enhanced security. For more information, see [AWS Documentation](#).

---

### Specifying Settings for New IAM Role

[This step applies if you have selected the Create new IAM role option]

At the **Role Settings** step of the wizard, specify the following settings:

1. **In the AWS role name field**, specify a name that will be used to create the IAM role in AWS.
   
   Consider the following limitations:

   - The specified name must be unique within one AWS account.
   - The following characters are not supported: `\ / " [ ] : | < > ; ? * & .`
   - The length of the name must not exceed 63 characters.

   For more information on IAM role name requirements, see [AWS Documentation](#).

2. Select check boxes next to permission sets that must be granted to the IAM role:
   
   - **Service role** — select this check box to grant permissions sufficient to launch worker instances.
Policy role — select this check box to grant permissions sufficient to perform backup.

The IAM role with this permission set will allow you to back up any instance or VPC configuration within the AWS account.

Repository role — select this check box to grant permissions sufficient to add Amazon S3 buckets as backup repositories.

The IAM role with this permission set will allow you to add as a backup repository any Amazon S3 bucket within the AWS account.

TIP

If you want the IAM role to have granular permissions, do not select any of the check boxes (for example, if you want the IAM role to have permissions only on specific EC2 instances). In this case, after the IAM role is created, you can grant the necessary permissions to it in the AWS Management Console. To learn how to grant permissions to IAM roles, see Appendix B. Creating IAM Policies in AWS.

3. Provide one-time access keys of an IAM user that is authorized to create IAM roles in the AWS account.

The specified access keys determine in which AWS account the role will be created. For example, if you specify access keys of an IAM user from the initial AWS account, the IAM role will be created in the initial AWS account and will have permissions on AWS services and resources of the initial account.

The IAM user must have the following permissions:

```
"iam:AttachRolePolicy",
"iam:CreatePolicy",
"iam:CreatePolicyVersion",
"iam:CreateRole",
"iam:GetAccountSummary",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
"iam:ListAttachedRolePolicies",
"iam:ListPolicyVersions",
"iam:UpdateAssumeRolePolicy"
```
NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.
Editing IAM Role Settings

For each IAM role added to Veeam Backup for AWS, you can modify the IAM role settings:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > IAM Roles**.
3. Select the check box next to an IAM role whose settings you want to edit.
4. Click **Edit**.
5. Complete the **Edit IAM Role** wizard.
   a. To provide a new name and description for the IAM role, follow the instructions provided in section **Adding IAM Roles** (step 2).
   b. To edit the IAM role settings, follow the instructions provided in section **Adding IAM Roles** (step 3).
   c. At the **Summary** step of the wizard, review summary information and click **Finish**.
Checking IAM Role Permissions

It is recommended that you run the IAM role permission check before you perform any operation to avoid the operation failure. For example, after you specify an IAM role in worker instance settings, you can check whether permissions of this IAM role are sufficient to launch worker instances. You can also run the permission check after you make changes in your AWS account and want to ensure that permissions granted to the IAM role remain sufficient.

To run the permission check for an IAM role, do the following:

1. Switch to the Configuration page.
2. Navigate to Accounts > IAM Roles.
3. Select an IAM role and click Check AWS Permissions.

Veeam Backup for AWS will display the AWS Permission Check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

To let Veeam Backup for AWS grant the missing permissions:

1. In the AWS Permission Check window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

The IAM user must have the following permissions:

```
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"
```

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. To make sure that the missing permissions have been successfully granted, click **Recheck**.
Removing IAM Roles

You can remove an IAM role from Veeam Backup for AWS if it is no longer used to perform data protection and disaster recovery operations.

**IMPORTANT**
You cannot remove an IAM role that is still used to get access to AWS resources or is specified in settings of any configured backup policy.

To remove an IAM role, do the following:

1. Switch to the Configuration page.
2. Navigate to Accounts > IAM Roles.
3. Select the IAM role and click Remove.
4. In the Remove IAM Role window, click Yes to acknowledge the operation.
Managing Permissions

Veeam Backup for AWS controls access to its functionality with the help of user roles. A role defines what operations users can perform and what range of data is available to them in Veeam Backup for AWS.

There are 3 user roles that you can assign to users working with Veeam Backup for AWS. Actions a user can perform depend on the role.

- **Portal Administrator** — can perform all configuration actions and can also act as a Portal Operator and Restore Operator.
- **Portal Operator** — can create and manage backup policies, manage the protected data and perform all restore operations.
- **Restore Operator** — can only perform restore operations.

The following table describes the functionality available to users with different roles in the Veeam Backup for AWS UI.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Functionality</th>
<th>Portal Administrator</th>
<th>Portal Operator</th>
<th>Restore Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>Dashboard</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Infrastructure</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td>Backup policies</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Protected Data</strong></td>
<td>Restore</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>File-level restore</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Session Log</strong></td>
<td>Session log</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td></td>
<td>Stop session execution</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Accounts</strong></td>
<td>IAM roles, SMTP accounts, Portal Users</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Repositories</strong></td>
<td>Backup repositories</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Workers</strong></td>
<td>Worker instances</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Tab</td>
<td>Functionality</td>
<td>Portal Administrator</td>
<td>Portal Operator</td>
<td>Restore Operator</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>General settings</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Licensing</strong></td>
<td>Licensing</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Support Information</strong></td>
<td>Updates and logs</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Adding User Accounts

To manage access to Veeam Backup for AWS, you can create local user accounts or add user accounts of your identity provider. To be able to retrieve user identities from the identity provider, you must first configure single sign-on settings.

To add a Veeam Backup for AWS user account, do the following:

1. Switch to the Configuration page.
3. Click Add.
4. Complete the Add Account wizard:
   a. At the Account Type step of the wizard, choose whether you want to create a new Veeam Backup for AWS user or to retrieve a user identity from your identity provider.
   b. At the Account Info step of the wizard, specify a name and description for the user account. An account name cannot be admin; can contain only lowercase Latin letters, numeric characters, underscores and dashes. You can use the dollar sign ($) as the last character of the name. The maximum length of the name is 32 characters, the maximum length of the description is 255 characters.

   **IMPORTANT**

   If you have selected the Identity Provider account option at step 4a, the name specified for a user account must match the value of an attribute that the identity provider will send to Veeam Backup for AWS to authenticate the user. For more information, see Configuring SSO Settings.

   c. At the General Settings step of the wizard, select a role for the user account. For more information on user roles, see Managing Permissions.

   If you have selected the Veeam Backup for AWS account option at step 4a, specify a password for the new Veeam Backup for AWS user account.

   d. At the Summary step of the wizard, review summary information and click Finish.
Editing User Account Settings

For each user account added to the Veeam Backup for AWS configuration database, you can modify the settings of the account:

1. Switch to the Configuration page.
3. Select the user account and click Edit.
4. Complete the Edit Account wizard.
   a. At the Account Info step of the wizard, edit a description of the user account.
   b. At the General Settings step of the wizard, select a new role for the user account.
   c. At the Summary step of the wizard, review summary information and click Finish.
Changing User Passwords

For Veeam Backup for AWS user accounts, you can change the password specified while creating the account:

**IMPORTANT**
You cannot change the password for a user account whose user identity was obtained from an identity provider.

1. Switch to the Configuration page.
3. Select the user account and click Change Password.
4. In the Change Password window, enter the currently used password, enter and confirm a new password, and then click Change.
Configuring Multi-Factor Authentication

Multi-factor authentication (MFA) in Veeam Backup for AWS is based on the Time-based One-Time Password (TOTP) method that requires users to verify their identity by providing a temporary six-digit code sent by an authentication application to a trusted device.

**IMPORTANT**
You cannot enable MFA for a user account whose user identity was obtained from an identity provider.

Enabling MFA

To enable MFA for a user account, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts > Portal Users**.
3. Select the user account and click **Enable MFA**.
4. Follow the instructions provided in the **MFA Settings** window:
   a. Install an authentication application on a trusted device.
   b. To associate the authentication application with the authorization server, scan the displayed QR code using the camera of the trusted device.
   c. Enter a verification code generated by the authentication application.
   d. Click **Apply**.

**NOTE**
Only Google Authenticator is fully supported by Veeam Backup for AWS.
Disabling MFA

To disable MFA for a user account, select the account on the Portal Users tab and click Disable MFA.
Managing Backup Repositories

Veeam Backup for AWS uses Amazon S3 buckets as target locations for EC2 instance image-level backups, additional copies of Amazon VPC backups, indexes of EFS file systems and Veeam Backup for AWS configuration backups. To instruct Veeam Backup for AWS to store backups in a specific Amazon S3 bucket, configure a backup repository. For more details, see Adding Backup Repositories.

To communicate with the backup repository, Veeam Backup for AWS uses the Veeam Data Mover — the service running on a worker instance that is responsible for data processing and transfer. When a backup policy addresses the backup repository, the Veeam Data Mover establishes a connection with the repository enabling data transfer. To let the Veeam Data Mover access the target Amazon S3 bucket, Veeam Backup for AWS uses permissions of an IAM role specified in backup repository settings.
Adding Backup Repositories

You can use only existing Amazon S3 buckets as targets for backup repositories. Before you add a backup repository, check limitations for backup repositories.

To add a backup repository, complete the following steps:

1. Launch the Add Repository wizard.
2. Specify a backup repository name and description.
3. Configure backup repository settings.
4. Enable data encryption for the backup repository.
5. Finish working with the wizard.
Step 1. Launch Add Repository Wizard

To launch the **Add Repository** wizard, do the following:

1. **Switch** to the **Configuration** page.
2. **Navigate** to **Repositories**.
3. **Click Add**.
Step 2. Specify Repository Name and Description

At the **Info** step of the wizard, specify a name and description for the new backup repository. The name must be unique in Veeam Backup for AWS; the maximum length of the name is 125 characters; the maximum length of the description is 1024 characters.
Step 3. Configure Repository Settings

At the Settings step of the wizard, configure settings for the backup repository:

1. In the IAM role section, specify an IAM role whose permissions Veeam Backup for AWS will use to access the target Amazon S3 bucket. For more information on permissions required for the IAM role, see Repository IAM Role Permissions.

   For an IAM role to be displayed in the IAM role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the Add Repository wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.

2. In the Location section, do the following:
   a. Specify an Amazon S3 bucket where you want to store backups.
      i. Click the Choose bucket link.
      ii. In the Choose bucket window, select the Amazon S3 bucket that will be used as a target location for backups, and click Apply.

         For an Amazon S3 bucket to be displayed in the Bucket list, it must be created within an AWS account to which the specified IAM role belongs. To learn how to create Amazon S3 buckets, see AWS Documentation.

         It may take some time for Veeam Backup for AWS to retrieve information about existing Amazon S3 buckets from AWS. To speed up the data collection process, click Rescan.

   IMPORTANT

   If you have any S3 Lifecycle configuration associated with the selected Amazon S3 bucket, limit the scope of lifecycle rules applied to Amazon S3 objects in the bucket so that no rules are applied to backup files created by Veeam Backup for AWS. Otherwise, the files may be unexpectedly deleted or transitioned to another storage class, and Veeam Backup for AWS may not be able to access the files. For more information on managing S3 Lifecycle configurations, see AWS Documentation.

   b. Choose whether you want to use an existing folder inside the selected Amazon S3 bucket or to create a new one to group backup files stored in the bucket.

      To use an existing folder, select the Use existing folder option and click Choose folder. In the Choose folder window, select the necessary folder and click Select.

      For a folder to be displayed in the Folder list, it must have been created by any backup appliance as a repository (either existing or already removed from the backup infrastructure) in the selected Amazon S3 bucket.
IMPORTANT

If you select an existing folder for storing backup files, mind the following:

- The folder must not be specified as a backup repository on multiple backup appliances simultaneously. Retention sessions running on different backup appliances may corrupt backup files stored in the folder, which may result in unpredictable data loss.
- The created backup repository will have the storage class that has been specified when creating the folder. You cannot change the storage class for the repository.
- If encryption at the repository level is enabled for the selected folder, you must provide a password or an encryption key for this folder at step 4 of the wizard.
- If the selected folder already contains backups created by the Veeam backup service, Veeam Backup for AWS will import the backed-up data to the configuration database. You can then use this data to perform all disaster recovery operations described in section Performing Restore.

By default, Veeam Backup for AWS applies retention settings saved in the backup metadata to the imported backups. However, if the selected folder contains backups of resources that you plan to protect by a backup policy with the created repository specified as a backup target, Veeam Backup for AWS will rewrite the saved retention settings and will apply to the imported backups new retention settings configured for that backup policy.

- To create a new folder, select the Create new folder option and specify a name for the new folder. The maximum length of the name is 125 characters; the dash (/) character is not supported.

  c. [This step applies only if you have selected the Create new folder option] From the Storage class drop-down list, select a storage class for the backup repository:

- To store backups in a high-availability and high-performance storage class that you plan to access frequently, select S3 Standard.

- To store backups in a secure, durable and low-cost archive storage class that you plan to access infrequently, select S3 Glacier.

- To store backups in the lowest-cost archive storage class that you plan to access once or twice a year, select S3 Glacier Deep Archive.

For more information on Amazon S3 storage classes, see AWS Documentation.
NOTE

When you select the S3 Glacier or S3 Glacier Deep Archive storage class for a backup repository, Veeam Backup for AWS does not create any S3 Glacier vaults in your AWS environment — it assigns the selected storage class to backups stored in the repository. That is why the archived backups remain in Amazon S3 and cannot be accessed directly through the Amazon S3 Glacier service.
Step 4. Enable Data Encryption

At the **Options** step of the wizard, choose whether you want to encrypt backup files stored in the selected Amazon S3 bucket folder.

**IMPORTANT**

If you have selected an existing folder at the **Settings** step of the wizard, and if encryption is enabled for this folder at the repository level, you must provide the currently used password or an encryption key to let Veeam Backup for AWS access this folder and add it as a backup repository. You cannot change encryption settings while adding the repository. However, you will be able to edit the repository settings later.

To enable encryption for the backup repository, do the following:

1. Click **Edit Encryption Settings**.
2. In the **Encryption settings** window, set the **Enable encryption** toggle to **On**.
3. Choose whether you want to use a password or an AWS Key Management Service (KMS) key to encrypt the backed-up data. For more information on encryption algorithms, see [Backup Repository Encryption](#).
   - To use password encryption, select the **Use password encryption** option and specify a password that will be used to encrypt data.
   - To encrypt data using AWS KMS keys, select the **Use KMS encryption key** option and choose a KMS key from the **Encryption key** drop-down list.
     
     For a KMS key to be displayed in the list of available encryption keys, it must be created in the AWS Region where the selected Amazon S3 bucket is located, and the IAM role specified to access the bucket must have permissions to the key. For more information on permissions required for the IAM role, see [Repository IAM Role Permissions](#).
IMPORTANT

If you select the **Use KMS encryption key** option, mind the following:

- AWS managed keys cannot be used to encrypt repositories due to **AWS limitations**.
- Only symmetric KMS keys are supported.
- Do not disable KMS keys used to encrypt repositories, otherwise Veeam Backup for AWS will not be able to encrypt data, and backup policies that have encrypted repositories specified as backup targets will fail to complete successfully.
- Do not delete KMS keys used to encrypt repositories, otherwise Veeam Backup for AWS will not be able to decrypt data stored in these repositories.

If a KMS key is scheduled for deletion, it will acquire the **Pending deletion** state. In this case, Veeam Backup for AWS will raise the warning, and, during the following 7 days, you must either change the encryption settings for the backup repository in Veeam Backup for AWS or cancel the key deletion.

For more information on managing AWS KMS keys, see **AWS Documentation**.
Step 5. Finish Working with Wizard

At the Summary step of the wizard, it is recommended that you run the IAM role permission check before you click Finish.

To check whether the specified IAM role has all the required permissions, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column.

You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it:

1. In the Permission check window, click Grant.

2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

   The IAM user must have the following permissions:

   ```
   "iam:CreatePolicy",
   "iam:GetRole",
   "iam:GetPolicy",
   "iam:AttachRolePolicy"
   ```

   NOTE
   Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. After the required permissions are granted, close the Permission check window, review configuration information and click Finish.
As soon as you click **Finish**, Veeam Backup for AWS will start adding the backup repository to the infrastructure. To track the progress, select the **Go to Sessions** check box to proceed to the Sessions Log page.
Editing Backup Repository Settings

For each backup repository, you can modify settings configured while adding the repository to the Veeam Backup for AWS infrastructure:

**NOTE**
You cannot change an Amazon S3 bucket, folder and storage class for a backup repository.

1. Switch to the **Configuration** page.
2. Navigate to **Repositories**.
3. Select the check box next to the backup repository and click **Edit**.
4. Complete the **Edit Repository** wizard.
   a. To provide a new name and description for the backup repository, follow the instructions provided in section **Adding Backup Repositories** (step 2).
   b. To enable encryption for the repository or to change the encryption settings, follow the instructions provided in section **Adding Backup Repositories** (step 4).
   c. At the **Summary** step of the wizard, review summary information and click **Finish** to confirm the changes.

As soon as you click **Finish**, Veeam Backup for AWS will start modifying the backup repository settings. To track the progress, select the **Go to Sessions** check box to proceed to the **Sessions Log page**.
Removing Backup Repositories

You can remove backup repositories from the backup infrastructure. When you remove a repository, Veeam Backup for AWS unassigns the repository role from the folder in the Amazon S3 bucket so that this folder is no longer used as a backup repository.

**NOTE**

Even though the Amazon S3 bucket is no longer used as a backup repository, Veeam Backup for AWS preserves all backup files previously stored in the repository and keeps these files in Amazon S3. You can assign the Amazon S3 bucket to a new backup repository so that Veeam Backup for AWS imports the backed-up data to the configuration database. In this case, you will be able to perform all disaster recovery operations described in section **Performing Restore**.

If you no longer need the backed-up data, either delete it as described in section **Managing Backed-Up Data** before you remove the repository from the Veeam Backup for AWS infrastructure, or use the AWS Management Console to delete the data if the repository has already been removed.

To remove a backup repository, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Repositories**.
3. Select the check box next to the backup repository and click **Remove**.
4. In the **Remove Repository** window, click **Remove** to acknowledge the operation.

**IMPORTANT**

You cannot remove a backup repository that is used by any backup policy. Modify the settings of all the related policies to remove references to the repository, and then try removing the repository again. To learn how to modify the backup policy settings, see **Performing Backup**.
Managing Worker Instances

To perform most data protection and disaster recovery operations (such as creating and removing EC2 image-level backups, restoring backed-up data, EFS indexing), Veeam Backup for AWS uses worker instances. Each worker instance is launched in a specific AWS Region for the duration of the backup, restore and retention process. For more information on AWS Regions in which Veeam Backup for AWS launches worker instances to perform operations, see Architecture Overview.

**NOTE**

You can tell worker instances from other EC2 instances running in your environment by their names — all worker instances deployed by Veeam Backup for AWS to perform backup and restore operations have the same name — **VBA_Worker**, all worker instances deployed by Veeam Backup for AWS to perform EFS indexing have the same name — **EFS_Worker**.
Managing Worker Configurations

A configuration is a group of network settings that Veeam Backup for AWS uses to deploy worker instances in a specific AWS Region to perform data protection, disaster recovery, backup retention and EFS indexing operations. Veeam Backup for AWS deploys one worker instance per each AWS resource added to a backup policy, restore or retention task.

Depending on the performed operation, Veeam Backup for AWS launches worker instances in the following AWS accounts:

- Worker instances used for backup, retention and restore operations are launched in the Backup account — an AWS account to which an IAM role specified to launch worker instances belong.
  
  By default, Veeam Backup for AWS uses the Default Backup Restore role to launch worker instances. Therefore, the Backup account is an AWS account where the backup appliance belong. However, you can change the Backup account. To do that, specify an IAM role from another AWS account to launch worker instances as described in section Adding Configurations for Backup Account.

- Worker instances used to perform EFS indexing operations are launched in production accounts — same AWS accounts where the processed file systems belong. For more information, see Adding Configurations for Production Accounts.

Adding Configurations for Backup Account

To launch worker instances used for backup, retention and restore operations, Veeam Backup for AWS uses the default network settings of AWS Regions. However, to optimize infrastructure costs and to ensure better performance of backup, retention and restore processes, you can add worker configurations to specify network settings for each Availability Zone in which worker instances will be deployed. To do that:

- Specify an IAM role from the backup AWS account.
- Add worker configurations for specific AWS Regions.

Specifying IAM Role

By default, Veeam Backup for AWS uses permissions of the Default Backup Restore IAM role to launch worker instances. The role is preconfigured and has all the required permissions to launch worker instances within the initial AWS account.

You can specify a different IAM role, for example, if you want Veeam Backup for AWS to change the Backup account. Before you specify the necessary role, make sure it is added to Veeam Backup for AWS as described in section Adding IAM Roles.

To specify an IAM role for worker instances, do the following:

1. Open the Configuration page.
2. Navigate to Workers > Network.
3. At the Backup Accounts tab, click the link in the Service IAM role field.
4. In the Choose IAM Role window, select the necessary IAM role, and then click Apply.

**IMPORTANT**
Consider that if you change the specified IAM role, all configured worker instance settings will be automatically removed as soon as you specify another IAM role.
After you specify the IAM role, it is recommended that you check whether permissions of the specified IAM role are sufficient to launch worker instances. For information on how to check IAM role permissions, see Checking IAM Role Permissions. To learn what permissions must have the IAM role used to launch worker instances, see Service IAM Role Permissions.

### Adding Worker Configurations

For each Availability Zone in which worker instances will be launched, you can configure specific network settings:

1. In the **Worker configurations** section, click **Add**.
2. Complete the **Add Worker Configuration** wizard.
   a. At the **General** step of the wizard, select an AWS Region and Availability Zone for which you want to configure network settings.

**NOTE**

If you create the worker configuration that will be used to perform EC2 backup operations, you can select any Availability Zone in the specified AWS Region. Veeam Backup for AWS will still be able to perform the operations even if the selected zone will differ from the Availability Zone where the processed EC2 instances reside. For restore operations, the configuration must be created in the same Availability Zone where the restored EC2 instance will operate.

b. At the **Network** step of the wizard, select an Amazon VPC and a subnet to which you want to connect worker instances, and specify a security group that must be associated with the instances. For more information on Amazon VPC, subnets and security groups, see AWS Documentation.

Veeam Backup for AWS will apply the specified network settings to all worker instances that will be launched in the AWS Region and Availability Zone selected at the **General** step of the wizard.
**IMPORTANT**

When selecting a subnet and security group, consider the following:

- Security rules configured in the selected security group must allow direct network traffic to AWS resources. Proxy redirect and setting a proxy in the Veeam Backup for AWS configuration are not supported.
- By default, Veeam Backup for AWS uses public IPv4 addresses to communicate with worker instances. If the public IPv4 addressing attribute is disabled for the selected subnet, Veeam Backup for AWS will display a warning at the Summary step of the wizard. In this case, you must either enable public IPv4 addressing for the subnet, or configure the sqs, ssm, ec2messages and ssmmessages endpoints for it to let Veeam Backup for AWS use private IPv4 addresses. To learn how to configure endpoints, see Appendix C. Configuring Endpoints in AWS.
- If you select an Outpost subnet, backup and restore operations in the AWS Region to which the AWS Outpost is connected may fail to complete successfully. The issue occurs if the default worker instance type is not supported for the AWS Outpost. To work around the issue, change the default worker profiles as described in Managing Worker Profiles.

c. At the Summary step of the wizard, review summary information and click Finish.

**Related Topics:**

- Testing File-Level Restore
- Editing Configurations
- Removing Configurations

**Testing File-Level Restore**

Before you perform file-level restore, it is recommended that you run a file-level restore test. The file-level restore test allows you to check whether AWS Region network settings are configured properly to launch worker instances, and that you can access the file-level recovery browser from the local machine.

To run the file-level restore test for an AWS Region, do the following:

1. Open the Configuration page.
2. Navigate to **Workers > Network**.

3. In the **Worker configurations** section, select the necessary configuration, and then click **Test FLR**.

4. Wait until the status of the file-level restore test in the **FLR Status** column changes to **Running**, and then click the status.

   Veeam Backup for AWS will display the **FLR Test Log** window where you can track the progress and view the results of the test.

5. If network settings are configured properly for the AWS Region, Veeam Backup for AWS will launch the worker instance and display the link to the file-level recovery browser in the **FLR Test Log** window.

   a. To check that you can access the file-level recovery browser, click the displayed link.

   b. To finish the file-level restore test, click **End Test** in the file-level recovery browser.

   If you do not click **End Test** within 30 minutes after Veeam Backup for AWS displays the link to the file-level recovery browser, the file-level restore test will finish automatically with the **Warning** status.

   **TIP**

   If the file-level restore test finishes with the **Warning** or **Error** status, you can run the test again after fixing issues with the network settings. To do that, in the **FLR Status** column, click the status of the file-level restore test, and then, click **Start test** in the **FLR Test Log** window.

---

<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Message</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2020 5:47:00 PM</td>
<td>Success</td>
<td>Test FLR task eu-central-1 started at 06/12/2020 17:46:55</td>
<td></td>
</tr>
<tr>
<td>06/12/2020 5:47:00 PM</td>
<td>Running</td>
<td>Processing Test FLR eu-central-1.</td>
<td>18 minutes 9 seconds</td>
</tr>
<tr>
<td>06/12/2020 5:47:07 PM</td>
<td>Success</td>
<td>Preparing the worker VM.</td>
<td>7 minutes 59 seconds</td>
</tr>
<tr>
<td>06/12/2020 5:53:07 PM</td>
<td>Success</td>
<td>Configuring FLR worker</td>
<td>7 minutes 43 seconds</td>
</tr>
<tr>
<td>06/12/2020 6:02:51 PM</td>
<td>Success</td>
<td>S3 endpoint url: <a href="https://s3.eu-central-1.amazonaws.com">https://s3.eu-central-1.amazonaws.com</a> ...</td>
<td></td>
</tr>
</tbody>
</table>
Adding Configurations for Production Accounts

To launch worker instances used for EFS indexing operations, Veeam Backup for AWS selects the most appropriate network settings of AWS Regions in production accounts (for example, selects a VPC specified as a mount target for the processed file system). However, to optimize infrastructure costs and to ensure better performance of the processes, you can add worker configurations to specify network settings for each region in which worker instances will be deployed. You can add multiple worker configurations with different network settings per AWS Region.

To add a worker configuration:

1. Open the Configuration page.
2. Navigate to Workers > Network.
3. Switch to the Production Accounts tab.
4. In the Worker configurations section, click Add.
5. Complete the Add Worker Configuration wizard.
   
a. At the General step of the wizard, do the following:
   i. In the Account section, select an AWS account where file systems that you plan to index belong and specify an IAM role that will be used to access and list region network settings in the selected AWS account.

   NOTE

The selected IAM role will be used only to list network settings in the current wizard. The role whose permissions Veeam Backup for AWS will use to access the configured settings during indexing operations must be specified in the backup policy settings.

   ii. In the Region section, select an AWS Region and Availability Zone where EFS systems that you plan to index reside.

b. At the Network step of the wizard, select an Amazon VPC and a subnet to which you want to connect worker instances, and specify a security group that must be associated with the instances. For more information on Amazon VPC, subnets and security groups, see AWS Documentation.

Veeam Backup for AWS will apply the specified network settings to all worker instances that will be launched for EFS indexing of file systems that have mount targets in the selected VPC.
IMPORTANT

Consider the following:

- The selected security group must allow outbound access on 2049 and 443 ports. These ports are used by worker instances to mount file systems and to communicate with AWS services. Proxy redirect and setting a proxy in the Veeam Backup for AWS configuration are not supported.
- The DNS resolution option must be enabled for the selected VPC. For more information, see AWS Documentation.
- By default, Veeam Backup for AWS uses public access to communicate with worker instances. That is why the public IPv4 addressing attribute must be enabled for the selected subnet, the selected VPC must have an internet gateway attached, and VPC and subnet route tables must have routes that direct internet-bound traffic to this internet gateway.

If you want worker instances to operate in the private network, configure private endpoints for it to let Veeam Backup for AWS use private IPv4 addresses. To learn how to configure endpoints, see Appendix C. Configuring Endpoints in AWS.

c. At the Summary step of the wizard, review summary information and click Finish.

Editing Configurations

You can edit worker configurations added for AWS Regions:

1. Open the Configuration page.
2. Navigate to Workers > Network.
3. Switch to the necessary tab.
4. Select the worker configuration and click Edit.
5. Complete the Edit Worker Configuration wizard:
   a. To modify the VPC and subnet to which the related worker instances are connected, and to change the security group associated with the instances, follow the instructions provided in section Adding Configurations for Backup Account (step 2.b) or in section Adding Configurations for Production Accounts (step 5.b).
b. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

**NOTE**

If any worker instances are currently launched in the selected AWS Region, the changes will be applied only when Veeam Backup for AWS removes the instances from the infrastructure (that is, when the running backup or restore process completes).

**Removing Configurations**

Veeam Backup for AWS allows you to permanently remove worker configurations from the infrastructure if you no longer need them. When you remove a worker configuration, Veeam Backup for AWS does not remove currently running worker instances that have been created based on this configuration — these instances are removed only when the related operations complete.

To remove a worker configuration from the Veeam Backup for AWS infrastructure, do the following:

1. Open the **Configuration** page.
2. Navigate to **Workers > Network**.
3. Switch to the necessary tab.
4. Select the worker configuration and click **Remove**.
NOTE

If there are any worker instances created based on the selected configuration that are currently involved in a backup or restore process, these instances will be removed only when the process completes.
Managing Worker Profiles

Worker profiles are instance types of worker instances that Veeam Backup for AWS deploys in a specific AWS Region to perform backup, restore, archive and health check operations. Veeam Backup for AWS launches one worker instance per each AWS resource added to a backup policy or restore task. The profile of each deployed worker instance is selected based on the performed operation and the size of EBS volumes attached to the processed instance.

There are 4 types of worker profiles in Veeam Backup for AWS:

- **Small profile** — a profile that is used for EC2 backup and restore operations if the EBS volume size of the processed instance is less than 1024 GB.
- **Medium profile** — a profile that is used for EC2 backup and restore operations if the EBS volume size of the processed instance is 1024 GB - 1250 GB.
- **Large profile** — a profile that is used for EC2 backup and restore operations if the EBS volume size of the processed instance is more than 1250 GB.
- **Archiving profile** — a profile that is used for creating archived backups.

Out of the box, Veeam Backup for AWS comes with the default set of worker profiles where the small profile is c5.large, the medium profile is c5.xlarge, the large profile is c5.2xlarge, and the archiving profile is c5.2xlarge. However, to boost operational performance, you can add custom sets of worker profiles to specify instance types of worker instances that will be deployed in different regions.

**IMPORTANT**

You cannot change the default worker profile used to launch worker instances that perform EC2 file-level restore, EFS indexing and retention operations — the default instance sizes of these worker instances are described in Architecture Overview. If you want to use a specific instance size for these worker instances, open a support case.

Adding Profiles

For each AWS Region in which worker instances will be launched, you can add a custom set of worker profiles:

1. Open the Configuration page.
2. Navigate to Workers > Profile and click Add.
3. Complete the Add Worker Profiles wizard.
   a. At the Regions step of the wizard, select regions for which you want to specify worker profiles and click Add.
   b. At the Worker Profiles step of the wizard, choose profiles that will be used to deploy workers in the selected regions. To help you choose, tables in the Choose instance type section will provide information on the number of vCPU cores and the amount of system RAM for each available instance type.

For the full description of instance types that can be used to deploy EC2 instances in AWS, see AWS Documentation.
At the **Summary** step of the wizard, review summary information and click **Finish**.

As soon as you click **Finish**, Veeam Backup for AWS will create a separate set of worker profiles for each of the selected regions.

---

### Editing Profiles

For each set of worker profiles created for an AWS Region, you can modify settings specified while creating the profile set:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Profiles**.
3. Select the profile set and click **Edit**.
4. Complete the **Edit Worker Profiles** wizard:
   a. To change profiles that will be used to deploy workers in the selected region, follow the instructions provided in section **Adding Profiles** (step 3.b).
   b. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.
If there are any worker instances that are currently involved in a backup or archive backup process in the selected region, the changes will be applied only when the process completes.

Removing Profiles

Veeam Backup for AWS allows you to permanently remove sets of worker profiles if you no longer need them. When you remove a profile set, Veeam Backup for AWS does not remove currently running worker instances that have been created based on this set — these instances are removed only when the related operations complete.

To remove a profile set from the Veeam Backup for AWS infrastructure, do the following:

1. Switch to the Configuration page.
2. Navigate to Workers > Profiles.
3. Select the profile set and click Remove.
Add worker profiles that will be used to launch worker instances for backup, restore, and archive operations in AWS regions.

By default, the following profiles are used:
- Small profile (c6.large) is used if the processed S3 volume size is less than 16TB
- Medium profile (c5.large)
- Large profile (c5.xlarge)
- Archiving profile

If you remove the worker profile, the default profile settings will be used to launch worker instances in the selected region.

<table>
<thead>
<tr>
<th>Region</th>
<th>Small Profile</th>
<th>Medium Profile</th>
<th>Large Profile</th>
<th>Archiving Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>c6.large</td>
<td>c5.large</td>
<td>c5.xlarge</td>
<td>c5.xlarge</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>c6.large</td>
<td>c5.large</td>
<td>c5.xlarge</td>
<td>c5.xlarge</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>c6.large</td>
<td>c5.large</td>
<td>c5.xlarge</td>
<td>c5.xlarge</td>
</tr>
<tr>
<td>E.U. West (London)</td>
<td>c5.large</td>
<td>c5.xlarge</td>
<td>c5.xlarge</td>
<td>c5.xlarge</td>
</tr>
<tr>
<td>E.U. West (Paris)</td>
<td>c5.large</td>
<td>c5.xlarge</td>
<td>c5.xlarge</td>
<td>c5.xlarge</td>
</tr>
</tbody>
</table>
Configuring General Settings

Veeam Backup for AWS allows you to configure general settings that are applied to all performed operations and deployed infrastructure components.

- Define for how long obsolete snapshots and session records must be retained.
- Provide certificates to secure connections between Veeam Backup for AWS infrastructure components.
- Configure notification settings for automated delivery of reports.
- Change the time zone set on the backup appliance.
- Configure single sign-on settings to retrieve user identities from an identity provider.
Configuring Global Retention Settings

You can configure global retention settings to specify for how long the following data must be retained in the configuration database:

- Obsolete snapshots and replicas
- Session records

Configuring Retention Settings for Obsolete Snapshots and Replicas

If an instance is no longer processed by a backup policy (for example, it was removed from the backup policy or the backup policy no longer exists), its cloud-native snapshots and snapshot replicas become obsolete. Retention policy settings configured when creating backup policies do not apply to obsolete snapshots — these snapshots are removed from the configuration database according to their own retention settings.

**NOTE**
Global retention settings apply to all cloud-native snapshots and snapshot replicas created by the Veeam backup service. If an instance is still processed by a backup policy, but some of its cloud-native snapshots and snapshot replicas are older than the number of days (or months) specified in the global retention settings, these cloud-native snapshots and snapshot replicas will be removed from Veeam Backup for AWS.

To configure retention settings for obsolete snapshots and replicas, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Settings > Retention**.
3. In the **Obsolete snapshots retention** section, select one of the following options:
   - Select the **Never** option if you do not want Veeam Backup for AWS to remove obsolete snapshots and replicas.
   - Select the **After** option to specify the number of days (or months) during which Veeam Backup for AWS must keep obsolete snapshots in the configuration database. The number must be between 90 and 36135.
     
     If you select this option, Veeam Backup for AWS will first wait for the specified period of time after an instance stops being processed by a backup policy, and then will remove its obsolete snapshots from the configuration database as soon as the period is over.
4. Click **Save**.

**NOTE**
When Veeam Backup for AWS removes an obsolete snapshot from the configuration database, it also removes the snapshot from the AWS infrastructure.

Configuring Retention Settings for Session Records

Veeam Backup for AWS stores records for all sessions of performed data protection and disaster recovery operations in the configuration database on the additional data disk attached to the backup appliance. These session records are removed from the configuration database according to their own retention settings.
To configure retention settings for session records, do the following:

1. In the **Session logs retention** section, select one of the following options:
   
   - Select the **Keep all session logs** option if you do not want Veeam Backup for AWS to remove session records.
   
   - Select the **Keep session logs only for last** option if you want to specify the number of days (or months) during which Veeam Backup for AWS must keep session records in the configuration database.

   If you select this option, Veeam Backup for AWS will remove all session records that are older than the specified time limit.

2. Click **Save**.

**IMPORTANT**

Retaining all session records in the configuration database may overload the data disk. By default, the disk comes with 20 GB of storage capacity. If you choose not to remove session records at all, consider increasing the disk space to avoid runtime problems.
Configuring Global Email Notification Settings

You can specify email notification settings for automated delivery of backup policy results and daily reports. Every daily report contains cumulative statistics for all backup policy and snapshot retention sessions run within the past 24-hour period.

To connect an SMTP server that will be used for sending email notifications:

1. Switch to the Configuration page.
2. Navigate to Settings > E-mail.
3. Select the Enable e-mail notifications check box.
4. In the SMTP Server field, specify a DNS name or an IP address of the SMTP server. All email notifications (including test messages) and daily reports will be sent by this SMTP server.
5. Click Advanced to specify an account that will be used when authenticating against the SMTP server and to configure other connection settings.

   In the Advanced SMTP Options window:
   a. In the Port field, specify a communication port for SMTP traffic. The default SMTP port is 25.
   b. In the Timeout field, specify a connection timeout for responses from the SMTP server.
   c. For an SMTP server with SSL/TLS support, select the Connect using SSL check box to enable SSL data encryption.
   d. If your SMTP server requires authentication, select the This SMTP server requires authentication check box and choose the necessary account from the Log on as drop-down list.

      For an account to be displayed in the Log on as list, it must be added to the configuration database as described in section Adding SMTP Accounts. If you have not set up an account beforehand, click Add and follow the steps of the Add Account wizard.
   e. Click Apply.
6. In the From field, enter an email address of the notification sender. This email address will be displayed in the From field of notifications.
7. In the To field, enter an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.

   For each particular policy, you can specify additional recipients. For more information on backup policies, see Performing Backup.

   NOTE

If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for AWS will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.

8. In the Subject field, specify a subject for notifications. You can use the following runtime variables:
   a. %JobName% — a backup policy name.
   b. [%JobResult%] — a backup policy result.
   c. (%ObjectCount% instances) — the number of instances in a backup policy.
- **%Issues%** — the number of instances in a backup policy that encountered any issues (errors and warnings) while being processed.

9. In the **Notify me immediately about policy** section, choose whether you want to receive email notifications in case backup policies complete successfully, complete with warnings or complete with errors.

10. To receive daily reports, select the **Send daily report at** check box and specify the exact time when the reports will be sent.

11. Click **Save**.

**TIP**

Veeam Backup for AWS allows you to send a test message to check whether you have configured all settings correctly. To do that, click **Send Test E-mail**. A test message will be sent to the specified email address.

---

### Adding SMTP Accounts

To add an account that will be used to connect to an SMTP server, do the following:

1. Switch to the **Configuration** page.

2. Navigate to **Accounts > SMTP Accounts**.

3. Click **Add**.

   Complete the **Add Account** wizard.

   a. At the **Account Name** step of the wizard, specify a name and description for the SMTP account. The name must be unique in Veeam Backup for AWS and the length of the name must not exceed 255 characters. The description length must not exceed 255 characters.

   b. At the **Account** step of the wizard, specify credentials of a user account that has permissions to access the SMTP server. Veeam Backup for AWS will use the specified credentials to authenticate against the SMTP server.
c. At the **Summary** step of the wizard, review summary information and click **Finish**.

---

**Editing SMTP Accounts**

For each SMTP account, you can modify the settings configured while adding the account:

1. Switch to the **Configuration** page.
2. Navigate to **Accounts** > **SMTP Accounts**.
3. Select the check box next to the necessary SMTP account and click **Edit**.

Complete the **Edit Account** wizard.

   a. To provide a new name and description for the account, follow the instructions provided in section **Adding SMTP Accounts** (step 4).

   b. To specify credentials of another user account to be used to authenticate against the SMTP server, follow the instructions provided in section **Adding SMTP Accounts** (step 5).
Replacing Security Certificates

To establish secure data communications between the backup appliance and web browsers running on user workstations, Veeam Backup for AWS uses Transport Layer Security (TLS) certificates.

**IMPORTANT**

When updating to Veeam Backup for AWS version 5.0, mind that only the TLS v1.3 certificates are now supported. Veeam Backup for AWS will automatically recreate all previously generated self-signed certificates.

When you install Veeam Backup for AWS, it automatically generates a default self-signed certificate. You can replace this default certificate with your own self-signed certificate or with a certificate obtained from a Certificate Authority (CA). To replace the currently used TLS certificate, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > Certificates.
3. Click Replace Web Certificate.
   
   Complete the New Certificate Wizard.

   a. At the Certificate Source step of the wizard, do the following:
      
      - Select the **Recreate a self-sign certificate** option if you want to replace the existing certificate with a new self-signed certificate automatically generated by Veeam Backup for AWS.
      
      - Select the **Upload certificate** option if you want to upload a certificate that you obtained from a CA or generated using a 3rd party tool.

   b. [This step applies only if you have selected the Upload certificate(s) option] At the Upload certificate(s) step of the wizard, browse to the certificate that you want to install, and provide a password for the certificate file if required.

**NOTE**

Only .PFX and .P12 certificate files are supported.

   c. At the Summary step of the wizard, review summary information and click Finish. To allow Veeam Backup for AWS to discover the newly installed certificate, restart the backup appliance.
NOTE

If you have recreated the self-signed certificate, the browser from which you will try to access Veeam Backup for AWS next time will display a warning notifying that the connection is untrusted (although it is secured with SSL). To eliminate the warning, import the self-signed certificate to user workstations.
Changing Time Zone

Veeam Backup for AWS runs daily reports and performs all data protection and disaster recovery operations according to the time zone set on the backup appliance. Since the backup appliance is deployed on an EC2 instance in Amazon EC2, the time zone is set to Coordinated Universal Time (UTC) by default. However, you can change the time zone if required. For example, you may want the time on the backup appliance to match the time on the workstation from which you access Veeam Backup for AWS.

To change the time zone set on the backup appliance:

1. Switch to the Configuration page.
2. Navigate to Settings > Time Zone.
3. Select the necessary time zone from the Time zone drop-down list.
4. Click Save.

**NOTE**

It is not recommended to change the time zone if any data protection or disaster recovery session is currently running. Wait for all the running sessions to complete or stop them manually — and then change the time zone.
Configuring SSO Settings

Veeam Backup for AWS supports single sign-on (SSO) authentication based on the SAML 2.0 protocol. SSO authentication scheme allows a user to log in to different software systems with the same credentials using the identity provider service.

To configure SSO settings for Veeam Backup for AWS, complete the following steps:

1. Switch to the **Configuration** page.
2. Navigate to **Settings > Identity Provider**.
3. In the **Identity Provider Configuration** section, import identity provider settings from a file obtained from your identity provider:
   a. Click **Upload Metadata**.
   b. In the **Upload Identity Provider Configuration** window, click **Browse** to locate the file with the identity provider settings.
   c. Click **Upload**.
4. Forward the service provider authentication settings to the identity provider — to obtain the settings, in the **Veeam Backup for AWS Configuration** section, click **Download**. Veeam Backup for AWS will download a metadata file with the service provider authentication settings to your local machine.
   Alternatively, you can copy the service provider settings manually:
   a. Click **Copy Link** in the **SP Entity ID / Issuer** field.
   b. Click **Copy Link** in the **Assertion Consumer URL** field.
5. [Optional] If you want to sign and encrypt authentication requests sent from Veeam Backup for AWS to the identity provider, select a certificate with a private key that will be used to sign and encrypt the requests:
   a. In the **Veeam Backup for AWS Configuration** section, click **Select** in the **Certificate** field.
   b. In the **Upload Veeam Backup certificate** window, click **Browse** to locate the certificate file. In the **Password** field, specify a password used to open the file.
   c. Click **Upload**.

**NOTE**
Only .PFX and .P12 certificate files are supported.

After you configure SSO settings, you can add user accounts that will be able to log in to Veeam Backup for AWS using single sign-on. For more information, see **Adding User Accounts**.
IMPORTANT

To authenticate a user whose identity has been received from the identity provider, Veeam Backup for AWS redirects the user to the identity provider portal. After the user logs in to the portal, the identity provider sends a SAML authentication response to Veeam Backup for AWS. The SAML response must contain the Username attribute to allow Veeam Backup for AWS to identify the user. The attribute value must match the user name that you specify when creating the user account.

If your identity provider does not send the Username attribute by default, you must create a claim rule on the identity provider side to send this attribute in the SAML authentication response to the Veeam Backup for AWS request.
Performing Configuration Backup and Restore

You can back up and restore the configuration database that stores data collected from Veeam Backup for AWS for the existing backup policies, protected EC2 instances, RDS resources, EFS file systems and VPC configurations, created worker instance configurations and profiles, added IAM roles and users, logged session records and so on. If the backup appliance goes down for some reason, you can reinstall it and quickly restore its configuration from a backup. You can also use a configuration backup to migrate the configuration of one backup appliance to another backup appliance in the AWS infrastructure.

It is recommended that you regularly perform configuration backup for every backup appliance present in the AWS infrastructure. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead costs in case any problems with the backup appliances occur.

You can run configuration backup manually on demand, or instruct Veeam Backup for AWS to do it automatically on a regular basis.
Performing Configuration Backup Manually

While performing configuration backup, Veeam Backup for AWS exports data from the configuration database and saves it to a backup file in a backup repository. To back up the configuration database of the backup appliance manually, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > Configuration Backup.
3. In the Overview section, click Take Backup Now.
4. In the Create Manual Backup window, select a repository where the configuration backup will be stored, and click Create.

For a backup repository to be displayed in the Repository list, it must be added to Veeam Backup for AWS as described in section Adding Backup Repositories. The Repository list shows only backup repositories of the S3 Standard storage class that have encryption enabled.

As soon as you click Create, Veeam Backup for AWS will start creating a new backup file in the selected repository. To track the progress, click Go to Sessions in the Session Info window to proceed to the Session Logs page.

**TIP**

Once Veeam Backup for AWS creates a successful configuration backup, you can click Export Last Backup to download the backup file and then use it to restore configuration data.
Performing Configuration Backup Automatically

While performing configuration backup, Veeam Backup for AWS exports data from the configuration database and saves it to backup files in a backup repository. To instruct Veeam Backup for AWS to back up the configuration database of the backup appliance automatically by schedule, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > Configuration Backup.
3. In the Backup Schedule section, set the Enable scheduling toggle to On.
4. Click the link in Repository field, and select a repository where configuration backups will be stored in the Choose Repository window.
   
   For a backup repository to be displayed in the list of available repositories, it must be added to Veeam Backup for AWS as described in section Adding Backup Repositories. The list shows only backup repositories of the S3 Standard storage class that have encryption enabled.

5. In the Keep restore points for field, specify the number of days for which you want to keep restore points in a backup chain in the selected backup repository.
   
   If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the backup chain.

6. In the Create daily backup at field, choose whether configuration backups will be created every day, on weekdays (Monday through Friday), or on specific days.

7. Click Save.
Exporting Configuration Backup Data

Once Veeam Backup for AWS creates a successful configuration backup, you can export the configuration backup file and use it to restore configuration data on another backup appliance.

To export the configuration backup file, do the following:

1. Switch to the Configuration page.
2. Navigate to Settings > Configuration Backup.
3. Use one of the following options:
   a. To export the last successful configuration backup:
      i. In the Overview section, click Export Last Backup.
      ii. In the Export Last Backup window, specify a password that will be used to encrypt the exported file, provide a hint for the specified password, and click Export.
   b. To export a specific configuration backup file:
      i. In the Configuration restore section, click Available Restore Points.
      ii. In the Available Restore Points window, select the necessary backup and click Export Backup.
      iii. In the Export Backup window, specify a password that will be used to encrypt the exported file, provide a hint for the specified password, and click Export.

As soon as you click Export, Veeam Backup for AWS will save the exported backup file to the default download directory on the local machine.
Restoring Configuration Data

Veeam Backup for AWS offers restore of the configuration database that can be helpful in the following situations:

- The configuration database got corrupted, and you want to recover data from a configuration backup.
- You want to roll back the configuration database to a specific point in time.
- The backup appliance got corrupted, and you want to recover its configuration from a configuration backup.
- The backup appliance went down, and you want to apply its configuration to a new backup appliance.

**IMPORTANT**
Before you start the restore process, stop all policies that are currently running.

To restore the configuration database, do the following:

1. Launch the Configuration Restore wizard.
2. Choose a backup file.
3. Review the backup file info.
4. Choose restore options.
5. Track the restore progress.
6. View the results of verification steps.
7. Finish working with the wizard.
Step 1. Launch Configuration Restore Wizard

To launch the **Configuration Restore** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Settings > Configuration Backup**.
3. In the **Configuration restore** section, click **Restore**.
Step 2. Choose Backup File

At the **Backup File** step of the wizard, choose whether you want to use an exported backup file or a backup file stored in a backup repository.

- If you want to use a file stored in a backup repository, select the **Use backup file from repository** option and do the following:
  
  a. Click the link in the **Repository** field, and use the list of available repositories in the **Choose repository** window to select the repository where the configuration backup file is stored.

  For a backup repository to be displayed in the list of available repositories, it must be added to Veeam Backup for AWS as described in section **Adding Backup Repositories**. The repository list shows only backup repositories that store configuration backup files.

  b. Click the link in the **Backup file** field, and select the necessary file in the **Choose backup file** window.

- If you want to use a file that was exported from this or another backup appliance, select the **Use imported backup file** option, and do the following:

  a. Click the link in the **Backup file** field.

  b. In the **Import backup file** window, browse to the necessary backup file, provide a password that was used to encrypt the file, and click **Import**.

**IMPORTANT**

The size of an uploaded backup file must not exceed 250 MB. To upload a file of a bigger size, open a support case.
Step 3. Review Backup File Info

Veeam Backup for AWS will analyze the content of the selected backup file and display the following information:

- **File information** — the date and time when the backup file was created.
- **Product information** — the version of Veeam Backup for AWS that was installed on the initial backup appliance and the version of the File-Level Recovery service that was running on the appliance.

**IMPORTANT**

Configuration restore is not supported if the current version of Veeam Backup for AWS installed on the backup appliance is later than the version saved in the configuration backup file.

- **Product configuration** — configuration data saved in the file (such as number of existing backup policies, added IAM roles and repositories, logged session records and so on).

At the **File Content** step of the wizard, review the provided information and click **Next** to confirm that you want to use the selected file to restore the configuration data.
Step 4. Choose Restore Options

By default, Veeam Backup for AWS restores only configuration data for the existing infrastructure components, created backup policies and configured global settings. At the Restore Options step of the wizard, you can choose whether you want to restore session logs, user accounts of the initial backup appliance and VPC configuration backups as well.

**IMPORTANT**

After you click Restore, the restore process will start. You will not be able to halt the process or edit the restore settings.
Step 5. Track Restore Progress

Veeam Backup for AWS will display the results of every step performed while executing the configuration restore. At the Restore step of the wizard, wait for the restore process to complete and click Next.
Step 6. View Configuration Check Results

After the restore process is over, Veeam Backup for AWS will run a number of verification checks to confirm that the configuration data has been restored successfully. At the Configuration Check step of the wizard, wait for the verification checks to complete and check whether Veeam Backup for AWS encountered any configuration issues.

If Veeam Backup for AWS encounters an issue while performing a verification check, the Result column will display a description of the issue, and the Action column will provide instructions on how to resolve it. For example, to resolve the issue with IAM role permissions, do the following:

1. In the Action column, click View in the Role permissions field.
2. In the IAM role permissions window, review IAM roles that are missing permissions required to perform operations, and choose one of the following options:
   - If you do not plan to use an IAM role to perform Veeam Backup for AWS operations, skip the notification and, after the configuration restore operation completes, specify a new role in the repository, policy and worker settings shown in the Used As column.
   - If you want to grant the missing permissions to an IAM role in the AWS Management Console, select the necessary role and click Export Missing Permissions to download the full list of missing permissions as a single JSON policy document.
   - If you want to instruct Veeam Backup for AWS to assign the missing permissions to an IAM role, select the necessary role and click Grant.

In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Grant.

The IAM user must have the following permissions:

```json
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"
```

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.

After you resolve all issues, click Recheck to ensure the backup appliance is now fully functional, and click Next.
IMPORTANT

Make sure that restored repositories will not be managed by multiple backup appliances simultaneously. Retention sessions running on different backup appliances may corrupt backup files stored in the repositories, which may result in unpredictable data loss.
Step 7. Finish Working with Wizard

At the Summary step of the wizard, click **Finish** to finalize the process of configuration data restore.
Viewing Available Resources

After you create a backup policy to protect a specific type of AWS resources (EC2 instances, RDS resources or EFS file systems), Veeam Backup for AWS rescans AWS Regions specified in the policy settings and populates the resource list on the Resources page with all resources of that type residing in these regions. If an AWS Region is no longer specified in any configured backup policy, Veeam Backup for AWS removes all resources residing in the region from the list of available resources.

The Resources page displays AWS resources that can be protected by Veeam Backup for AWS. Each resource is represented with a set of properties, such as:

- **Instance** or **Name** — the name of the resource.
- **Instance ID** or **File System ID** — the unique identification number of the resource.
- **Instance Size** or **Source Size** — the size of the resource storage.

**NOTE**

Veeam Backup for AWS does not show sizes of Aurora DB clusters due to AWS REST API limitations.

- **AWS Account** — the AWS account where the resource belong.
- **Region** — the AWS Region where the resource resides.
- **Backup Policy** — the name of the backup policy that protects the resource (if any).
- **Restore Points** — the number of restore points created for the resource (if any).
- **Last Backup** — the date and time of the latest restore point created for the resource (if any).
- **Destination** — types of restore points created for the resource (if any).

On the Resources page you can also perform the following actions:

- Manually create cloud-native snapshots of RDS and EC2 instances and backups of EFS file systems. For more information, see sections Creating EC2 Snapshots Manually, Creating RDS Snapshots Manually and Creating EFS Backups Manually.

- Add resources to existing backup policies. For more information, see Adding Resources to Policy.
Adding Resources to Policy

If you want to protect additional resources by configured backup policies, you can either edit the backup policy settings, or quickly add the resources to the backup policies on the Resources tab.

To add a resource to a backup policy, do the following:

1. Navigate to Resources.
2. Switch to the necessary tab and select the resource that you want to protect by a backup policy.
   For a resource to be displayed in the list of available resources, an AWS Region where the resource resides must be specified in any of configured backup policies that protects this kind of resources, and the IAM role specified in the backup policy settings must have permissions to access the resource.
3. Click Add to Policy.
4. In the Add to Policy window:
   a. Choose the backup policy that must protect the selected resource and click Add.
   For a backup policy to be displayed in the list of available policies, an AWS Region where the selected resource resides must be specified in the policy settings, and the IAM role used by Veeam Backup for AWS for this backup policy must have permissions to access the selected resource.
   b. Review the configured settings and click OK.
Performing Backup

With Veeam Backup for AWS, you can protect data in the following ways:

- **Create cloud-native snapshots of EC2 instances and RDS resources**
  A cloud-native snapshot of an EC2 instance includes point-in-time snapshots of EBS volumes attached to the processed instance. Snapshots of EBS volumes (also referred to as EBS snapshots) are taken using native AWS capabilities.

  A cloud-native snapshot of a DB instance includes a storage volume snapshot of the instance. Snapshots of DB instances (also referred to as DB snapshots) are taken using native AWS capabilities.

  A cloud-native snapshot of an Aurora DB cluster includes a storage volume snapshot of the cluster that backs up the entire cluster and not just individual databases. Snapshots of Aurora DB clusters (also referred to as DB cluster snapshots) are taken using native AWS capabilities.

- **Replicate cloud-native snapshots to a remote site**
  By default, cloud-native snapshots are stored only in the AWS Region where the processed instance resides. For enhanced data safety, you can instruct Veeam Backup for AWS to create copies of cloud-native snapshots and store them in any other AWS Region within any AWS account. You can also combine the snapshot replication functionality with various data recovery options to migrate instance data between AWS Regions and AWS accounts.

- **Create image-level backups of EC2 instances**
  In addition to cloud-native snapshots, you can protect your EC2 instances with image-level backups. An image-level backup captures the whole image of the processed EC2 instance (including instance configuration, OS data, application data and so on) at a specific point in time. The backup is saved to a backup repository in the native Veeam format.

- **Create backups and backup copies of your EFS file systems**
  An Amazon EFS file system backup captures the whole image of the EFS file system (including file system configuration, files, directories and so on) at a specific point of time. EFS backups are taken using native AWS capabilities.

  By default, EFS backups are stored only in the AWS Region where the processed file system resides. For enhanced data safety, you can instruct Veeam Backup for AWS to create copies of these backups and store them in any other AWS Region within the same AWS account. You can also combine the backup copy functionality with various data recovery options to migrate file system data between AWS Regions.

- **Create backups of your VPC configuration**
  An Amazon VPC configuration backup captures the whole image of a VPC configuration of an AWS account (including multiple VPC configuration settings and components) at a specific point in time. By default, the VPC configuration backup is stored in the Veeam Backup for AWS database. For enhanced data safety, you can instruct Veeam Backup for AWS to create copies of Amazon VPC configuration backups and store them in a backup repository.

**IMPORTANT**

Veeam Backup for AWS does not support backup of the following VPC configuration components: VPC Traffic Mirroring, AWS Network Firewall, VPC Flow Logs, carrier gateways, customer IP pools, and core networks in route tables.
To schedule data protection tasks to run automatically, create backup policies. You will be able to run the backup policies on demand and manually perform backup of EC2 instances, RDS resources and EFS file systems. To learn how to perform backup manually, see sections Creating EC2 Snapshots Manually, Creating RDS Snapshots Manually, Creating EFS Backups Manually.

**TIP**

You can perform advanced data protection operations with image-level backups from the Veeam Backup & Replication console. For details, see the External Repository section in the Veeam Backup & Replication User Guide.
How Backup Works

Veeam Backup for AWS does not install agent software inside instances to retrieve data. To back up resource data, Veeam Backup for AWS uses native AWS capabilities. During every backup session, Veeam Backup for AWS creates a cloud-native snapshot (for an EC2 instance and RDS resource) or a cloud-native backup (for an EFS file system) for each AWS resource added to a backup policy. The cloud-native snapshot is further used to create a snapshot replica (for an EC2 instance and RDS resource) in another AWS Region or another AWS account and an image-level backup (only for an EC2 instance), the cloud-native backup (for an EFS file system) is further used to create a backup copy in another AWS Region.

To protect Amazon VPC configurations, Veeam Backup for AWS retrieves configuration data through API and saves this data to the configuration database. You can also instruct Veeam Backup for AWS to store copies of VPC configuration backups in a backup repository.

In this section:

- EC2 Backup
- RDS Backup
- EFS Backup
- VPC Configuration Backup
- Retention Policy
EC2 Backup

Veeam Backup for AWS performs EC2 backup in the following way:

1. Veeam Backup for AWS creates snapshots of EBS volumes that are attached to the processed EC2 instance.

2. EBS snapshots are assigned AWS tags upon creation. Keys and values of AWS tags contain encrypted metadata that helps Veeam Backup for AWS identify the related EBS snapshots and treat them as a single unit — a cloud-native snapshot.

3. If you enable snapshot replication for the backup policy, Veeam Backup for AWS copies cloud-native snapshots to the target AWS Region and AWS account specified in the backup policy settings.

4. If you enable image-level backup for the backup policy, Veeam Backup for AWS performs the following operations:
   a. Launches a worker instance in an AWS Region where the processed EC2 instance resides.
      By default, Veeam Backup for AWS uses the default network settings of AWS Regions to launch worker instances. However, you can add specific worker configurations. For more information on worker instances, see Managing Worker Instances.
   b. Re-creates the EBS volumes from the cloud-native snapshot created at step 1 and attaches them to the worker instance.
      Note that the cloud-native snapshot used as a source for image-level backup is not a temporary snapshot — when the backup session completes, this snapshot remains in the snapshot chain and is deleted later according to the specified policy scheduling settings. For more information, see CBT Impact on Snapshot Retention.
   c. Reads data from the EBS volumes on the worker instance, transfers the data to a backup repository and stores it in the native Veeam format.
      To reduce the amount of data read from EBS volumes, Veeam Backup for AWS uses the changed block tracking (CBT) mechanism: during incremental backup sessions, Veeam Backup for AWS compares the new cloud-native snapshot with the previous one and reads only those data blocks that have changed since the previous backup session. If CBT cannot be used, Veeam Backup for AWS reads all data from the re-created EBS volumes. For more information, see Changed Block Tracking.
   d. When the backup session completes, removes the worker instance from Amazon EC2.

5. If you enable the backup archiving mechanism, Veeam Backup for AWS performs the following operations:
   a. Launches a worker instance in an AWS Region where a backup repository storing backed-up data resides.
   b. Retrieves data from the backup repository and transfers it to the archive repository.
   c. When the archive session completes, removes the worker instance from Amazon EC2.

NOTE

Veeam Backup for AWS encrypts and compresses data saved to backup repositories. For more information on data encryption, see Enabling Data Encryption.

d. When the backup session completes, removes the worker instance from Amazon EC2.

182 | Veeam Backup for AWS | User Guide
Snapshot Chain

During every backup session, Veeam Backup for AWS creates a cloud-native snapshot for each instance added to the backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots that Veeam Backup for AWS takes using native AWS capabilities.

A sequence of cloud-native snapshots created during a set of backup sessions makes up a snapshot chain. Veeam Backup for AWS creates the snapshot chain in the following way:

1. During the first backup session, Veeam Backup for AWS creates a snapshot that contains all instance data and saves it in the AWS Region where the processed instance resides. This snapshot becomes a starting point in the snapshot chain.
   
The creation of the first snapshot may take significant time to complete since Veeam Backup for AWS copies the whole image of the instance.

2. During subsequent backup sessions, Veeam Backup for AWS creates snapshots that contain only those data blocks that have changed since the previous backup session.
   
The creation of subsequent snapshots typically takes less time to complete, compared to the first snapshot in the chain. Note, however, that the completion time still depends on the amount of processed data.
   
   For more information on how incremental snapshots work, see AWS Documentation.

Each cloud-native snapshot in the snapshot chain contains metadata. Metadata stores information about the protected instance and the backup policy that created the snapshot. Veeam Backup for AWS uses metadata to identify snapshots created by the Veeam backup service, to detect outdated snapshots, and to load the configuration of source instances during recovery operations, and so on.

Cloud-native snapshots act as independent restore points for backed-up instances. If you remove any snapshot, it will not break the snapshot chain — you will still be able to roll back instance data to any existing restore point.

The number of cloud-native snapshots kept in a snapshot chain is defined by retention policy settings. For details, see Snapshot Retention.

NOTE

Cloud-native snapshots created manually are not included into the snapshot chain. Therefore, these snapshots are not removed automatically according to retention policy settings. For information on how to remove them, see section Managing Backed-Up Data.

Snapshot Replica Chain

Snapshot replicas are copies of cloud-native snapshots that Veeam Backup for AWS creates during backup sessions. If you enable snapshot replication for a backup policy, Veeam Backup for AWS will make a copy of the initially created cloud-native snapshot and save it to the target AWS Region in the target AWS account specified in backup policy settings. Snapshot replicas created in the target AWS Region during a set of backup sessions make up a snapshot replica chain.
Veeam Backup for AWS creates and maintains the snapshot replica chain in the same way as the regular snapshot chain:

- The first snapshot replica of the processed instance becomes a starting point in the snapshot replica chain.
- Snapshot replicas created during subsequent backup sessions store only those data blocks that have changed since the previous backup session.

## Backup Chain

If you enable image-level backups for an EC2 backup policy, Veeam Backup for AWS creates a new backup file in a backup repository during every backup session. A sequence of backup files created during a set of backup sessions makes up a backup chain.

The backup chain includes backup files of the following types:

- **Full** — a full backup file stores a copy of the full EC2 image.
- **Incremental** — incremental backup files store incremental changes of EC2 images.

To create a backup chain for an EC2 instance protected by a backup policy, Veeam Backup for AWS implements the forever forward incremental backup method:

1. During the first backup session, Veeam Backup for AWS copies the full EC2 image and creates a full backup file in the backup repository. The full backup file becomes a starting point in the backup chain.
2. During subsequent backup sessions, Veeam Backup for AWS copies only those data blocks that have changed since the previous backup session, and stores these data blocks to incremental backup files in the backup repository. The content of each incremental backup file depends on the content of the full backup file and the preceding incremental backup files in the backup chain.

![Backup Chain Diagram](image)

Full and incremental backup files act as restore points for backed-up EC2 instances that let you roll back instance data to the necessary state. To recover an EC2 instance to a specific point in time, the chain of backup files created for the instance must contain a full backup file and a set of incremental backup files dependent on the full backup file.

If some file in the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backup files from the backup repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backup files in the backup repository. For more information, see [EC2 Backup Retention](#).

## Changed Block Tracking

The changed block tracking (CBT) mechanism allows Veeam Backup for AWS to reduce the amount of data read from processed EBS volumes, and to increase the speed and efficiency of incremental backups:

- During a full backup session, Veeam Backup for AWS reads only written data blocks, while unallocated data blocks are filtered out.
- During an incremental backup session, Veeam Backup for AWS reads only those data blocks that have changed since the previous backup session.
To detect unallocated and changed data blocks, CBT relies on EBS Direct APIs.

1. During the first (full) backup session, Veeam Backup for AWS creates a cloud-native snapshot of an EC2 instance. To do that, Veeam Backup for AWS sends API requests to access the content of the snapshot and to detect unallocated data blocks.

2. During subsequent sessions, new cloud-native snapshots are created. Veeam Backup for AWS sends API requests to access and to compare the content of the snapshot created during the previous backup session and the snapshot created during the current backup session. This allows Veeam Backup for AWS to detect data blocks that have changed since the previous backup session.

Limitations for Changed Block Tracking

Veeam Backup for AWS cannot use CBT for EC2 instances that reside in AWS Regions where EBS Direct APIs are not available.

If CBT cannot be used, Veeam Backup for AWS reads the whole content of processed EBS volumes and compares it with backed-up data that already exists in the backup repository. In this case, the completion time of incremental backups may occur to grow.

Archive Backup Chain

If you enable backup archiving for a backup policy, Veeam Backup for AWS creates a new backup file in an archive repository during every archive session. A sequence of backup files created during a set of archive sessions makes up an archive backup chain.

The archive backup chain includes backup files of the following types:

- **Full**—a full archive backup file stores a copy of the full EC2 instance image.
- **Incremental**—incremental archive backup files store incremental changes of the EC2 instance image.

To create an archive backup chain for a EC2 instance protected by a backup policy, Veeam Backup for AWS implements the forever forward incremental backup method:

1. During the first archive session, Veeam Backup for AWS detects backed-up data that is stored in the full backup file and all incremental backup files existing in the standard backup chain, creates a full archive backup file with all the data, and copies this file to the archive repository. The full archive backup file becomes a starting point in the archive chain.

2. During subsequent archive sessions, Veeam Backup for AWS checks the standard backup chain to detect data blocks that have changed since the previous archive session, creates incremental archive backup files with only those changed blocks, and copies these files to the archive repository. The content of each incremental archive backup file depends on the content of the full archive backup file and the preceding incremental archive backup files in the archive backup chain.

Full and incremental archive backup files act as restore points for backed-up EC2 instances that let you roll back instance data to the necessary state. To recover an EC2 instance to a specific point in time, the chain of backup files created for the instance must contain a full archive backup file and a set of incremental archive backup files.
If some file in the archive backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backup files from the archive repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backup files in the archive repository. For more information, see Retention Policy for Archived Backups.
RDS Backup

Veeam Backup for AWS performs RDS backup in the following way:

1. Veeam Backup for AWS creates a storage volume snapshot of the processed DB instance (that is, a DB snapshot) or of the processed Aurora DB cluster (that is, a DB cluster snapshot).

   The snapshot is assigned AWS tags upon creation. Keys and values of AWS tags contain encrypted metadata that helps Veeam Backup for AWS identify the related snapshot. For the Aurora DB cluster metadata saved in AWS tags also contains information on every DB instance launched in the cluster.

2. If you enable snapshot replication for the backup policy, Veeam Backup for AWS copies the snapshot to the target AWS Region and AWS account specified in the backup policy settings.

   **NOTE**

   Snapshot replication is not supported for Aurora multi-master clusters.

Snapshot Chain

During every backup session, Veeam Backup for AWS creates a cloud-native snapshot for each instance added to the backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots that Veeam Backup for AWS takes using native AWS capabilities.

A sequence of cloud-native snapshots created during a set of backup sessions makes up a snapshot chain.

Veeam Backup for AWS creates the snapshot chain in the following way:

1. During the first backup session, Veeam Backup for AWS creates a snapshot that contains all instance data and saves it in the AWS Region where the processed instance resides. This snapshot becomes a starting point in the snapshot chain.

   The creation of the first snapshot may take significant time to complete since Veeam Backup for AWS copies the whole image of the instance.

2. During subsequent backup sessions, Veeam Backup for AWS creates snapshots that contain only those data blocks that have changed since the previous backup session.

   The creation of subsequent snapshots typically takes less time to complete, compared to the first snapshot in the chain. Note, however, that the completion time still depends on the amount of processed data.

   For more information on how incremental snapshots work, see AWS Documentation.

Each cloud-native snapshot in the snapshot chain contains metadata. Metadata stores information about the protected instance and the backup policy that created the snapshot. Veeam Backup for AWS uses metadata to identify snapshots created by the Veeam backup service, to detect outdated snapshots, and to load the configuration of source instances during recovery operations, and so on.

Cloud-native snapshots act as independent restore points for backed-up instances. If you remove any snapshot, it will not break the snapshot chain — you will still be able to roll back instance data to any existing restore point.
The number of cloud-native snapshots kept in a snapshot chain is defined by retention policy settings. For details, see Snapshot Retention.

**NOTE**

Cloud-native snapshots created manually are not included into the snapshot chain. Therefore, these snapshots are not removed automatically according to retention policy settings. For information on how to remove them, see section Managing Backed-Up Data.

**Snapshot Replica Chain**

Snapshot replicas are copies of cloud-native snapshots that Veeam Backup for AWS creates during backup sessions. If you enable snapshot replication for a backup policy, Veeam Backup for AWS will make a copy of the initially created cloud-native snapshot and save it to the target AWS Region in the target AWS account specified in backup policy settings. Snapshot replicas created in the target AWS Region during a set of backup sessions make up a snapshot replica chain.

Veeam Backup for AWS creates and maintains the snapshot replica chain in the same way as the regular snapshot chain:

- The first snapshot replica of the processed instance becomes a starting point in the snapshot replica chain.
- Snapshot replicas created during subsequent backup sessions store only those data blocks that have changed since the previous backup session.
Veeam Backup for AWS performs EFS backup in the following way:

1. Veeam Backup for AWS creates a cloud-native backup of the file system using AWS Backup service and saves this backup to the specified backup vault in the same AWS Region in which the source file system resides. The backup is assigned AWS tags upon creation. Keys and values of AWS tags contain encrypted metadata that helps Veeam Backup for AWS identify the related EFS file system backup.

2. If you configure the EFS backup policy to copy backup files to another AWS Region, Veeam Backup for AWS copies the created backup to the target AWS Region in the same AWS account.

3. If you enable EFS indexing in the backup policy settings, Veeam Backup for AWS performs the following operations:
   a. Launches a worker instance in an AWS Region in which the processed file system resides in an AWS account where the file system belong — that is, the production AWS account. By default, Veeam Backup for AWS selects the most appropriate network settings of AWS Regions in production accounts (for example, selects a VPC specified as a mount target for the processed file system). However, you can add specific worker configurations. For more information on worker instances, see Managing Worker Configurations.
   
   b. Mounts the source file system on the worker instance.

   c. Reads data from the file system using the worker instance, creates a catalog of files and folders (index) of the system, transfers the index to a backup repository and stores it in the native Veeam format.

   The EFS index is associated with the cloud-native backup created at step 1 and the backup copy created at step 2. However, if the indexing session does not complete by the time a new backup session starts, a new indexing session is not launched and Veeam Backup for AWS associates the created EFS index with 2 cloud-native backups and backup copies created by 2 backup sessions.

   d. When the indexing session completes, removes the worker instance from Amazon EC2.

**NOTE**

Veeam Backup for AWS encrypts and compresses data saved to backup repositories. For more information on data encryption, see Enabling Data Encryption.

**Backup Chain**

During every backup session, Veeam Backup for AWS creates an EFS backup for each EFS file system added to the backup policy. To take the backup Veeam Backup for AWS uses AWS Backup.
A sequence of cloud-native backups created during a set of backup sessions makes up a backup chain. Veeam Backup for AWS creates the backup chain in the following way:

1. During the first backup session, Veeam Backup for AWS creates a backup that contains all EFS file system data and saves it in the selected backup vault of the AWS Region where the processed file system resides. This backup becomes a starting point in the backup chain.

   The creation of the first backup may take significant time to complete since Veeam Backup for AWS copies the whole image of the EFS file system.

2. During subsequent backup sessions, Veeam Backup for AWS creates backups that contain only those data blocks (files and directories) that have changed since the previous backup session.

   The creation of subsequent backups typically takes less time to complete, compared to the first backup in the chain. Note, however, that the completion time still depends on the amount of processed data.

Each EFS backup in the backup chain contains metadata. Metadata stores information about the protected file system, the backup policy that created the backup, and the date, time and applied retention settings. Veeam Backup for AWS uses metadata to identify outdated backups, to load the configuration of source file systems during recovery operations, and so on.

EFS backups act as independent restore points for backed-up file systems. If you remove any backup, it will not break the EFS backup chain — you will still be able to roll back file system data to any existing restore point. The period of time during which EFS backups are kept in the EFS backup chain is defined by retention policy settings. For details, see EFS Backup Retention.

NOTE

EFS backups created manually are not included into the EFS backup chain. Therefore, these file system backups are not removed automatically according to retention policy settings. For information on how to remove them, see section Removing EFS Backups Created Manually.

EFS Backup Copy Chain

If you enable backup copying for a backup policy, Veeam Backup for AWS will make a copy of the initially created EFS backup and save it to the target AWS Region specified in the backup policy settings. In the target AWS Region, backup copies created during a set of backup sessions make up a backup copy chain.

Veeam Backup for AWS creates and maintains an EFS backup copy chain in the same way as a regular EFS backup chain:

- The first created backup copy of the processed instance becomes a starting point in the backup copy chain.
- Backup copies created during subsequent backup sessions store only those data blocks that have changed since the previous backup session.

Veeam Backup for AWS applies to an EFS backup copy chain the same retention settings as to the regular EFS backup chain.
EFS Indexing Chain

If you enable EFS indexing for a backup policy, Veeam Backup for AWS during each indexing session creates an index of the processed file system and associates the index with one or multiple restore points as described in section EFS Backup. In the target backup repository, EFS indexes created during a set of indexing sessions make up an indexing chain.

EFS indexes always contain full file catalogs of the processed file system. Therefore, if you delete any index from the backup repository, the index chain will not be corrupted but you may not be able to restore file and folders to a restore point associated with the deleted index using the file-level recovery browser. To learn how to perform file-level recovery, see Performing File-Level Restore.

The period of time during which EFS indexes are kept in the indexing chain is defined by time stamps that were saved in the index metadata when creating the indexes. For details, see EFS Backup Retention.
VPC Configuration Backup

Veeam Backup for AWS performs VPC configuration backup in the following way:

1. Veeam Backup for AWS sends API requests to AWS to retrieve the VPC configuration data, and saves this data in the Veeam Backup for AWS database.

   To back up VPC configurations of AWS Regions added to a backup policy, Veeam Backup for AWS uses permissions of an IAM role specified in the backup policy settings. The VPC configuration data is collected for the AWS account to which the specified IAM role belongs.

   Veeam Backup for AWS creates a configuration record for each pair of the AWS account and an AWS Region whose VPC configuration data is being backed up. Every time the VPC Configuration Backup policy runs, Veeam Backup for AWS updates the record to create a new restore point for the VPC configurations. For more information, see VPC Configuration Backup Chain.

2. If you configure the VPC Configuration Backup policy to copy backup files to a backup repository, Veeam Backup for AWS launches the Veeam Data Mover service on the backup appliance to copy the restore point to the target backup repository specified in the backup policy settings. In the repository, for each AWS account in which VPC configuration data has been backed up, Veeam Backup for AWS creates an individual folder with VPC configuration backup files.

Backup Chain

During every backup session, Veeam Backup for AWS creates a restore point with backed-up VPC configuration data for each AWS Region protected by the VPC Configuration Backup policy. The restore point contains metadata that includes information on the date and time when the policy ran, AWS Regions whose VPC configuration settings were backed up by the policy, and AWS accounts whose IAM roles were used to collect VPC configuration settings for each AWS Region.

A sequence of restore points created during a set of backup sessions makes up a VPC configuration backup chain for each configuration record.

You cannot delete specific restore points created for a configuration record — these points are removed automatically according to the specified retention policy settings. However, you can manually remove a configuration record with all restore points created for it, as described in section Removing VPC Configuration Backups.
Retention Policy

Cloud-native snapshots, snapshot replicas and image-level backups are not kept forever. They are removed according to retention policy specified in the backup schedule settings while creating a backup policy.

Depending on the data protection scenario, retention policy can be specified:

- **In restore points** – for cloud-native snapshots and snapshot replicas.
  The snapshot chain can contain only the allowed number of restore points. If the number of allowed restore points is exceeded, Veeam Backup for AWS removes the earliest restore point from the snapshot chain. For details, see EC2 and RDS Snapshot Retention.

- **In days/months/years** – for backups and archives.
  Restore points in the backup chain (either standard or archive) can be stored for the allowed period of time. If a restore point is older than the specified limit, Veeam Backup for AWS removes it from the backup chain. For details, see sections EC2 Backup Retention, EFS Backup Retention and VPC Configuration Backup Retention.

You can also specify global retention settings for obsolete snapshots and replicas. For details, see Configuring Global Retention Settings.

EC2 and RDS Snapshot Retention

For cloud-native snapshots and snapshot replicas, Veeam Backup for AWS retains the number of latest restore points defined in backup scheduling settings.

During every successful backup session, Veeam Backup for AWS creates a new restore point. If Veeam Backup for AWS detects that the number of restore points in the snapshot chain exceeds the retention limit, the earliest restore point is removed from the chain. For more information on the snapshot deletion process, see AWS Documentation.

NOTE

Mind that Veeam Backup for AWS does not apply retention policy to cloud-native snapshots created manually. For details on how to remove them, see section Managing Backed-Up Data.

EC2 Backup Retention

For image-level backups, Veeam Backup for AWS retains restore points for the number of days defined in backup scheduling settings.
To track and remove outdated restore points from a backup chain, Veeam Backup for AWS performs the following actions once a day:

1. Veeam Backup for AWS checks the configuration database to detect backup repositories that contain outdated restore points.

2. If an outdated restore point exists in a backup repository, Veeam Backup for AWS performs the following operations:
   
a. If the total size of backup files that must be deleted is more than 1 TB, launches a worker instance in an AWS Region where the backup repository is located to process a retention task. Otherwise, Veeam Backup for AWS processes the task on the backup appliance.
   
   By default, Veeam Backup for AWS uses the default network settings of AWS Regions to launch worker instances. However, you can add specific worker configurations. For more information on worker instances, see Managing Worker Instances.

   b. Transforms the backup chain in the following way:
      
i. Veeam Backup for AWS rebuilds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do that, Veeam Backup for AWS injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup ‘moves’ forward in the backup chain.

   
      ![Image of a flowchart showing the process]

   ii. Veeam Backup for AWS removes the earliest incremental backup file from the chain as redundant — this data has already been injected into the full backup file.

   
      ![Image of a flowchart showing the process]

3. Veeam Backup for AWS repeats step 2 for all other outdated restore points found in the backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full backup file, Veeam Backup for AWS ensures that the backup chain is not broken and that you will be able to recover your data when needed.

   ![Image of a flowchart showing the process]

4. If the worker instance was launched, Veeam Backup for AWS removes this worker instance from Amazon EC2 when the retention session completes.
NOTE

Mind the following:

- Veeam Backup for AWS can process maximum 5 retention tasks at a time. If the number of retention tasks that must be processed on the backup appliance is more than the specified limit, the tasks exceeding this limit are queued.
- Each worker instance can process only one retention task at a time. Veeam Backup for AWS simultaneously can launch maximum 5 worker instances that process retention tasks. If the number of retention tasks that must be processed on worker instances is more than the specified limit, the tasks exceeding this limit are queued.

CBT Impact on Snapshot Retention

If CBT is available, Veeam Backup for AWS does not remove the cloud-native snapshot used as a source for image-level backup from the snapshot chain until the next image-level backup session completes. Therefore, at some point you may discover that Veeam Backup for AWS ignores retention policy settings and keeps an additional restore point in the snapshot chain.

Consider the following example. You configured a backup policy to create cloud-native snapshots of your critical workloads 6 times a day (at 7:00 AM, 9:00 AM, 11:00 AM, 1:00 PM, 3:00 PM, and 5:00 PM) and to keep 2 daily snapshots in the snapshot chain. You also enabled creation of image-level backups 2 times a day (at 7:00 AM and 5:00 PM) and configured the retention policy settings to keep the backups in a backup repository for 7 days.

Veeam Backup for AWS will run the backup policy in the following way:

1. At 7:00 AM, the first backup session will create a cloud-native snapshot, and then will use this snapshot to create a full image-level backup.
2. From 9:00 AM to 3:00 PM, subsequent sessions will create only cloud-native snapshots.
   a. After the backup session runs at 11:00 AM, the length of the snapshot chain (3 restore points) will exceed the retention limit (2 restore points). The earliest snapshot, however, will not be removed as it will be used to track changed data at 5:00 PM when the next image-level backup creation is scheduled.
   b. After the backup session runs at 1:00 PM and 3:00 PM, Veeam Backup for AWS will remove the snapshots created at 9:00 AM and 11:00 AM. The length of the snapshot chain will remain 3 restore points.
3. At 5:00 PM, the backup session will create a new cloud-native snapshot. Veeam Backup for AWS will compare this snapshot with the one created at 7:00 AM to identify changed data blocks. After that, the backup session will create an incremental image-level backup based on the data obtained during the snapshot comparison.
4. After the snapshot comparison, Veeam Backup for AWS will apply the retention policy and remove from the chain the snapshot created at 7:00 AM (as it is no longer needed) and the snapshot created at 1:00 PM.

Retention Policy for Archived Backups

For archived backups, Veeam Backup for AWS retains restore points for the number of days defined in backup scheduling settings.

To track and remove outdated restore points from an archive backup chain, Veeam Backup for AWS performs the following actions once a day:

1. Veeam Backup for AWS checks the configuration database to detect archive backup repositories that contain outdated restore points.

2. If an outdated restore point exists in a archive backup repository, Veeam Backup for AWS performs the following operations:
   a. If the total size of backup files that must be deleted is more than 1 TB, launches a worker instance in an AWS Region where the backup repository is located to process a retention task. Otherwise, Veeam Backup for AWS processes the task on the backup appliance.
   
   By default, Veeam Backup for AWS uses the default network settings of AWS Regions to launch worker instances. However, you can add specific worker configurations. For more information on worker instances, see Managing Worker Instances.
   
   b. Transforms the archive backup chain in the following way:
      i. Veeam Backup for AWS rebuilds the full archive backup file to include the data of the incremental archive backup file that follows the full archive backup file. To do that, Veeam Backup for AWS injects into the full archive backup file data blocks from the earliest incremental archive backup file in the chain. This way, the full archive backup ‘moves’ forward in the archive backup chain.
   
   ii. Veeam Backup for AWS removes the earliest incremental archive backup file from the chain as redundant — this data has already been injected into the full archive backup file.
3. Veeam Backup for AWS repeats step 2 for all other outdated restore points found in the archive backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full archive backup file, Veeam Backup for AWS ensures that the archive backup chain is not broken and that you will be able to recover your data when needed.

4. If the worker instance was launched, Veeam Backup for AWS removes this worker instance from Amazon EC2 when the retention session completes.

**NOTE**

Mind the following:

- Veeam Backup for AWS can process maximum 5 retention tasks at a time. If the number of retention tasks that must be processed on the backup appliance is more than the specified limit, the tasks exceeding this limit are queued.
- Each worker instance can process only one retention task at a time. Veeam Backup for AWS simultaneously can launch maximum 5 worker instances that process retention tasks. If the number of retention tasks that must be processed on worker instances is more than the specified limit, the tasks exceeding this limit are queued.

### EFS Backup Retention

For EFS file system backups, Veeam Backup for AWS retains restore points for the period of time specified in backup scheduling settings.

During every successful backup session, Veeam Backup for AWS creates a restore point and saves the date, time and applied retention settings in the restore point metadata. If Veeam Backup for AWS detects that the period of time for which the restore point was stored exceeds the period specified in the retention settings, it automatically removes the restore point from the EFS backup chain. You can also remove unnecessary EFS backups manually as described in section Removing EFS Backups.

**NOTE**

Mind that Veeam Backup for AWS does not apply retention policy to EFS backups created manually. For details on how to remove them, see section Removing EFS Backups Created Manually.
**EFS Indexing Retention**

When creating an index, Veeam Backup for AWS writes to the index metadata a time stamp when the index must be deleted. The time stamp is defined by the retention specified in the backup policy settings for the first restore point with which the index is associated. If you change retention settings for the backup policy, time stamps of earlier created indexes will not change. However, even if the index must be deleted according to the time stamp, Veeam Backup for AWS will not delete the index until all associated restore points are removed from the Veeam Backup for AWS configuration database.

**VPC Configuration Backup Retention**

For VPC configuration backups, Veeam Backup for AWS retains restore points for the period of time specified in backup retention settings.

During every successful backup session, Veeam Backup for AWS creates a restore point and saves the date, time and the applied retention settings in the restore point metadata. If Veeam Backup for AWS detects that the period of time for which the restore point was stored exceeds the period specified in the retention settings, it automatically removes the restore point from the VPC configuration backup chain. You can also remove unnecessary VPC configuration backups manually as described in section Removing VPC Configuration Backups.

**NOTE**

Veeam Backup for AWS applies the retention settings configured for the VPC Configuration Backup policy both to VPC configuration backups stored in the Veeam Backup for AWS database and to VPC configuration backups stored in the backup repository selected for the policy. For VPC configuration backups stored in backup repositories that are not specified in the VPC Configuration Backup policy settings, Veeam Backup for AWS applies retention settings saved in the backup metadata.
Performing EC2 Backup

To produce cloud-native snapshots, snapshot replicas and image-level backups of EC2 instances, Veeam Backup for AWS runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

One backup policy can be used to process multiple EC2 instances residing in different regions within one AWS account, but you can back up each EC2 instance with one backup policy at a time. If an EC2 instance is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this EC2 instance from processing. For information on how to set a priority for a backup policy, see Setting Policy Priority.

For EC2 instances residing in any of the regions added to the backup policies, you can also take cloud-native snapshots manually when needed.

**IMPORTANT**

In Veeam Backup for AWS, you can protect only EC2 instances that run in VPCs. EC2-Classic instances are not supported. For details, see this Veeam KB article.
Creating EC2 Backup Policies

One backup policy can be used to process one or more instances within one AWS account. The scope of data that you can protect in an AWS account is limited by permissions of an IAM role that is specified in the backup policy settings.

Before you create an EC2 backup policy, check the following prerequisites:

- If you plan to create image-level backups of EC2 instances, backup infrastructure components that will take part in the backup process must be added to the backup infrastructure and configured properly. These include backup repositories and worker instances.
- If you plan to receive email notifications on backup policy results, configure SMTP server settings first. For details, see Configuring Global Email Notification Settings.
- If you plan to create transactionally consistent backups of EC2 instances, check the requirements for application-aware processing and guest scripting.

To create an EC2 backup policy, complete the following steps:

1. Launch the Add EC2 Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Enable guest processing.
5. Configure backup target settings.
6. Specify a schedule for the backup policy.
7. Enable AWS tags assigning.
8. Specify general settings.
10. Finish working with the wizard.
Step 1. Launch Add EC2 Policy Wizard

To launch the Add EC2 Policy wizard, complete the following steps.

1. Navigate to Policies > EC2.
2. Click Add.
Step 2. Specify Policy Name and Description

At the **Info** step of the wizard, use the **Name** and **Description** fields to specify a name for the new backup policy and to provide a description for future reference. The name must be unique in Veeam Backup for AWS; the maximum length of the name is 127 characters, the maximum length of the description is 255 characters.
Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify backup source settings:

1. **Select an IAM role whose permissions will be used to perform EC2 instance backup.**
2. **Select AWS Regions where EC2 instances that you plan to back up reside.**
3. **Select EC2 instances to back up.**
4. **Select EBS volumes of the selected EC2 instances to exclude from the backup policy.**
Step 3.1 Specify IAM Role

In the **IAM role** section of the **Sources** step of the wizard, you must specify an IAM role whose permissions will be used to access AWS services and resources, and to create cloud-native snapshots of EC2 instances. If you specify an IAM role created in another AWS account, the backup policy will process EC2 instances on which the specified IAM role has permissions in that AWS account.

For an IAM role to be displayed in the **IAM role** list, it must be added to Veeam Backup for AWS as described in *Adding IAM Roles*. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **Add Policy** wizard. To add an IAM role, click **Add** and complete the **Add IAM Role** wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click **Check Permissions**. Veeam Backup for AWS will display the **Permission check** window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the **Missing Permissions** column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

**TIP**

To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click **Export Missing Permissions**.

**IMPORTANT**

If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see *AWS Documentation*.

To let Veeam Backup for AWS grant the missing permissions:

1. In the **Permission check** window, click **Grant**.
2. In the **Grant permissions** window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click **Apply**.

The IAM user must have the following permissions:

```
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"
```

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. To make sure that the missing permissions have been successfully granted, click **Recheck**.
Step 3.2 Select AWS Regions

In the Specify region section of the Sources step of the wizard, select AWS Regions where EC2 instances that you plan to back up reside.

1. Click Choose regions.
2. In the Choose regions window, select the necessary AWS Regions from the Available Regions list, and click Add.
3. To save changes made to the backup policy settings, click Apply.
Step 3.3 Select EC2 Instances

In the Resources section of the Sources step of the wizard, specify the backup scope — select EC2 instances that Veeam Backup for AWS will back up:

1. Click Choose resources to protect.

2. In the Choose resource to protect window, choose whether you want to back up all EC2 instances from AWS Regions selected at step 3.2, or only specific EC2 instances.

   If you select the All resources option, Veeam Backup for AWS will regularly check for new EC2 instances launched in the selected regions and automatically update the backup policy settings to include these instances in the backup scope.

   If you select the Protect only following resources option, you must also specify the resources explicitly:

   a. Use the Resource type drop-down list to choose whether you want to add individual EC2 instances or AWS tags to the backup scope.

      If you select the Tag option, Veeam Backup for AWS will back up only those EC2 instances that reside in the selected regions under specific AWS tags.

   b. Use the search field to the right of the Resource type list to find the necessary resource, and then click Protect to add the resource to the backup scope.

      For a resource to be displayed in the list of available resources, it must reside in an AWS Region that has ever been specified in any backup policy. Otherwise, the only option to discover the available resources is to click Browse to select specific resources from the global list and to wait for Veeam Backup for AWS to populate the resource list.

   TIP

   You can simultaneously add multiple resources to the backup scope. To do that, click Browse to select specific sources from the global list, select check boxes next to the necessary EC2 instances or AWS tags in the list of available resources, and then click Protect.

   If the list does not show the resources that you want to back up, click Rescan to launch the data collection process. As soon as the process is over, Veeam Backup for AWS will update the resource list.

   If you add an AWS tag to the backup scope, Veeam Backup for AWS will regularly check for new EC2 instances assigned the added AWS tag and automatically update the backup policy settings to include these instances in the scope. However, this applies only to EC2 instances from the regions selected at step 3.2. If you select a tag assigned to EC2 instances from other regions, these instances will not be protected by the backup policy. To work around the issue, either go back to step 3.2 and add the missing regions, or create a new backup policy.

3. To save changes made to the backup policy settings, click Apply.
TIP

As an alternative to selecting the **Protect only following resources** option and specifying the resources explicitly, you can select the **All resources** option and exclude a number of resources from the backup scope. To do that, click **Choose resources to exclude** and specify the instances or tags that you do not want to protect — the procedure is the same as described for including resources in the backup scope.

Mind that if a resource appears both in the list of included and excluded resources, Veeam Backup for AWS will still not process the resource because the list of excluded resources has a higher priority.

---

[Image of the Veeam Backup for AWS interface showing the option to choose resources to protect or exclude.]
Step 3.4 Select EBS Volumes

In the **Volumes** section of the **Sources** step of the wizard, you can exclude from processing EBS volumes attached to the selected EC2 instances:

1. Set the **Exclude volumes** toggle to **On**.
2. In the **Choose volumes to exclude** window, choose whether you want to exclude system volumes of the selected EC2 instances from processing.
3. To exclude specific EBS volumes, specify the EBS volumes explicitly:
   a. Use the **Resource type** list to choose whether you want to exclude individual EBS volumes or AWS tags from the backup scope.
      - If you select the **Tag** option, Veeam Backup for AWS will exclude from processing only those EBS volumes that reside in the selected regions under specific AWS tags.
   b. Use the search field to the right of the **Resource type** list to find the necessary resource, and then click **Exclude** to exclude the resource from the backup scope.
      - For a resource to be displayed in the list of available resources, it must reside in an AWS Region that has ever been specified in any backup policy. Otherwise, the only option to discover the resources is to click **Browse to select specific resources from the global list** and to wait for Veeam Backup for AWS to populate the resource list.

**TIP**

You can simultaneously exclude multiple resources from the backup scope. To do that, click **Browse to select specific sources from the global list**, select check boxes next to the necessary EBS volumes or AWS tags in the list of available resources, and then click **Exclude**.

If the list does not show the resources that you want to exclude, click **Rescan** to launch the data collection process. As soon as the process is over, Veeam Backup for AWS will update the resource list.

If you exclude an AWS tag from the backup scope, Veeam Backup for AWS will regularly check for new EBS volumes assigned the excluded AWS tag and automatically update the backup policy settings to exclude these volumes from the scope.
4. To save changes made to the backup policy settings, click **Apply**.
Step 4. Specify Guest Processing Settings

If you back up EC2 instances that are currently running, at the Guest Processing step of the wizard, you can configure guest processing settings. These settings allow you to specify what actions Veeam Backup for AWS will perform when communicating with the instance guest OS.

Particularly, you can specify the following guest processing settings:

- **Enable application-aware processing.** For Windows EC2 instances running VSS-aware applications, you can enable application-aware processing to ensure that the applications will be able to recover successfully, without data loss.
  
  Application-aware processing is the Veeam technology based on Microsoft VSS. Microsoft VSS is responsible for quiescing applications on EC2 instances and creating a consistent view of application data. For more information on Microsoft VSS, see [Microsoft Docs](https://docs.microsoft.com).

- **Enable guest scripting.** For all processed EC2 instances, you can instruct Veeam Backup for AWS to run custom scripts on the instance before and after the backup operation. For example, for an EC2 instance running applications that do not support Microsoft VSS, Veeam Backup for AWS can execute a pre-snapshot script on the instance to quiesce these applications. This will allow Veeam Backup for AWS to create a transactionally consistent snapshot while no write operations occur on the instance volumes. After the snapshot is created, a post-snapshot script can start the applications again.

**Limitations and Requirements**

To be able to communicate with instance guest OSes, Veeam Backup for AWS uses the AWS Systems Manager (SSM) service. Thus, if you plan to enable guest processing for EC2 instances protected by the policy, you must consider the following:

- The backup appliance must have outbound internet access to the SSM service.

- EC2 instances for which you plan to enable guest processing must have the 443 network port opened for outbound internet access to ensure proper communication of Veeam Backup for AWS and the instance guest OSes.

- The IAM role used for EC2 instance backup must have the following permissions to communicate with the SSM service: `ssm:GetCommandInvocation`, `ssm:SendCommand`.

- EC2 instances for which you plan to enable guest processing must have the SSM Agent installed. If the SSM Agent is not installed on an EC2 instance, you can install the agent manually using the AWS Management Console.

  Note that the SSM Agent is preinstalled on EC2 instances launched from certain AMIs. For more information, see [AWS Documentation](https://docs.aws.amazon.com/AmazonSSM/latest/DeveloperGuide/)

For more information on the SSM service, see [AWS Documentation](https://docs.aws.amazon.com/AmazonSSM/latest/DeveloperGuide/).

**Enabling Application-Aware Processing**

To enable application-aware processing, at the Guest Processing step of the wizard, set the Enable application-aware snapshots toggle to **On**.
Limitations and Requirements for Application-Aware Processing

If you plan to instruct Veeam Backup for AWS to create transactionally consistent backups using application-aware processing, in addition to the limitations and requirements for guest processing, consider the following:

- Application-aware processing is available only for EC2 instances running Microsoft Windows Server 2008 R2 or later.
- EC2 instances for which you plan to enable application-aware processing must have VSS components installed. To learn how to download and install VSS components, see AWS Documentation.
- An IAM role with permissions required to take VSS-enabled snapshots must be created beforehand and attached to the processed EC2 instances. To learn how to create IAM roles for VSS-enabled snapshots, see AWS Documentation.

Enabling Guest Scripting

Before you enable guest scripting for processed EC2 instances, check limitations and requirements.

To enable guest scripting, at the Guest Processing step of the wizard, do the following:

- For EC2 instances running Linux OS, set the Scripting for Linux instances toggle to On.
  - The Specify scripting settings for Linux instances window will open.
- For EC2 instances running Microsoft Windows OS, set the Scripting for Microsoft Windows instances toggle to On.
  - The Specify scripting settings for Microsoft Windows instances window will open.

In the opened window, specify pre-snapshot and post-snapshot scripts that must be executed before and after the backup operation:

1. In the Pre-snapshot script section, do the following:
   a. In the Path in guest field, specify a path to the pre-snapshot script file on an EC2 instance.
b. In the **Arguments** field, specify additional arguments that must be passed to the script when the script is executed.

You can use runtime variables as arguments for the script. To see the list of available variables, click **Parameters**.

**NOTE**

Veeam Backup for AWS will run the script from the specified directory for all EC2 instances added to the backup policy. If you want to execute different scripts for different EC2 instances, ensure that script files uploaded to these instances are located under the same path and have the same name.

2. Repeat step 1 for post-snapshot scripts in the **Post-snapshot script** section.

3. In the **Additional options** section, choose whether you want to instruct Veeam Backup for AWS to:
   - Run scripts only while taking snapshot that will be used to create an image-level backup.
   - Proceed with snapshot creation even though scripts are missing on some of the processed instances.
   - Ignore exit codes returned while executing the scripts.

4. To save changes made to the backup policy settings, click **Apply**.

### Limitations and Requirements for Guest Scripting

If you plan to instruct Veeam Backup for AWS to run custom scripts on the processed EC2 instances, in addition to the **limitations and requirements for guest processing**, consider the following:

- Scripts must be created beforehand.
- For EC2 instances running Microsoft Windows OS, Veeam Backup for AWS supports scripts in the EXE, BAT, CMD, WSF, JS, VBS and PS1 file formats.
- For EC2 instances running Linux OS, Veeam Backup for AWS supports scripts in the SH file format.
- IAM instance profiles used to grant permissions for SSM to interact with the processed EC2 instances must be created beforehand and attached to these instances. To learn how to create IAM instance profiles for AWS Systems Manager, see AWS Documentation.
Step 5. Configure Backup Target Settings

By default, backup policies create only cloud-native snapshots of processed instances. At the **Targets** step of the wizard, you can enable the following additional data protection scenarios:

- Instruct Veeam Backup for AWS to replicate cloud-native snapshots to other AWS accounts or AWS Regions.
- Instruct Veeam Backup for AWS to create image-level backups.

Configuring Snapshot Replica Settings

If you want to replicate cloud-native snapshots to other AWS accounts or regions, do the following:

1. In the **Replicas** section of the **Targets** step of the wizard, set the **Replicate snapshots** toggle to **On**.

2. In the **Replication settings** window, configure the following mapping settings for each AWS Region where source instances reside:
   a. Select a source AWS Region in the list and click **Edit Region Mapping**.
   b. In the **Edit Region Mapping** window, specify the following settings:
      i. From the **Target account** drop-down list, select an IAM role whose permissions will be used to copy and store cloud-native snapshots in a target AWS Region.
         If you select an IAM role created in another AWS account, the cloud-native snapshot will be copied to a target AWS Region in that AWS account.
      ii. From the **Target region** drop-down list, select a target AWS Region to which Veeam Backup for AWS must copy cloud-native snapshots.
      iii. If you want to encrypt cloud-native snapshots copied to the target AWS Region, select the **Enable encryption** check box and choose the necessary KMS key from the **Encryption key** drop-down list. For a KMS key to be displayed in the list of available encryption keys, it must be stored in the target AWS Region, and the IAM role specified for the copy operation must have permissions to access the key. For more information on KMS keys, see AWS Documentation.
         Then, use the **Key usage** drop-down list to choose whether you want to encrypt snapshots for all volumes or only snapshots of the encrypted volumes.

   **NOTE**
   
   If the original EBS volume is encrypted, you must enable encryption for replicated snapshots, otherwise, the replication process will fail.

   iv. Click **Save**.

   **TIP**
   
   To configure mapping for all source AWS Regions at once, click **Set Mapping for All Regions** and specify settings as described in step 2.b.
c. To save changes made to the backup policy settings, click **Apply**.

## Related Resources

**AWS Key Management Service concepts**

**Configuring Image-Level Backup Settings**

If you want to create image-level backups of the selected EC2 instances, do the following:

1. In the **Backups** section of the **Targets** step of the wizard, set the **Enable backups** toggle to **On**.
2. In the **Repositories** window, select a standard repository where the created image-level backups will be stored, and click **Apply**.

For a backup repository to be displayed in the repository list, it must be added to Veeam Backup for AWS as described in section **Adding Backup Repositories**. The list shows only backup repositories of the **S3 Standard** storage class.

You can also enable the backup archiving mechanism to instruct Veeam Backup for AWS to store backed-up data in a low-cost, long-term archive storage:

1. Select the **Archives will be stored in** check box.
2. In the **Repositories** window, select an archive repository where the archived data will be stored, and click **Apply**.

For an archive repository to be displayed in the repository list, it must be added to Veeam Backup for AWS as described in section **Adding Backup Repositories**. The list shows only backup repositories of the **S3 Glacier or S3 Glacier Deep Archive** storage classes.

For more information on backup archiving, see **Enabling Backup Archiving**.
IMPORTANT

If you enable the backup archiving mechanism, consider that data encryption must be either enabled or disabled for both backup and archive repositories. This means that you cannot select an encrypted repository and an unencrypted repository in one backup policy. However, the selected repositories can have different encryption schemes (password and KMS encryption).
**Step 6. Specify Policy Scheduling Options**

You can instruct Veeam Backup for AWS to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the instances added to the backup policy will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for AWS allows you to create schedules of the following types:

- **Daily** — the backup policy will create restore points repeatedly throughout a day on specific days.
- **Weekly** — the backup policy will create restore points once a day on specific days.
- **Monthly** — the backup policy will create restore points once a month on a specific day.
- **Yearly** — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time — for more information, see [Enabling Harmonized Scheduling](#). Combining multiple schedule types together also allows you to archive backups — for more information, see [Enabling Backup Archiving](#).

**NOTE**

If you do not specify a backup schedule for the backup policy, you will need to start it manually to create EC2 instance snapshots and backups. For information on how to start backup policies, see [Starting and Stopping Policies](#).

### Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily schedule** toggle to **On** and click **Edit Daily Settings**.

2. In the **Create daily schedule** window, select hours when the backup policy will create cloud-native snapshots, snapshot replicas or image-level backups.

   If you want to protect EC2 instance data more frequently, you can instruct the backup policy to create multiple cloud-native snapshots per hour. To do that, click the link to the right of the **Snapshots** hour selection area, and specify the number of cloud-native snapshots that the backup policy will create within an hour.

**NOTE**

Veeam Backup for AWS does not create snapshot replicas and image-level backups independently from cloud-native snapshots. That is why when you select hours for snapshot replicas and image-level backups, the same hours are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see [EC2 Backup](#).

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on work days (Monday through Friday) or on specific days.

4. In the **Daily retention** section, configure retention policy settings for the daily schedule:

   - For cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.

     If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see [EC2 and RDS Snapshot Retention](#).
For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain. If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see EC2 Backup Retention.

5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly schedule** toggle to **On** and click **Edit Weekly Settings**.

2. In the **Create weekly schedule** window, select weekdays when the backup policy will create cloud-native snapshots, snapshot replicas or image-level backups.

**NOTE**

Veeam Backup for AWS does not create snapshot replicas and image-level backups independently from cloud-native snapshots. That is why when you select days to create snapshot replicas and image-level backups, the same days are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see EC2 Backup.

3. Use the **Create restore point at** drop-down list to schedule a specific time for the backup policy to run.

4. In the **Weekly retention** section, configure retention policy settings for the weekly schedule:

   o For cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.

   If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see EC2 and RDS Snapshot Retention.
For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.

If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see EC2 Backup Retention.

5. To save changes made to the backup policy settings, click Apply.

### Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Monthly schedule toggle to On and click Edit Monthly Settings.

2. [This step applies if you enabled backup archiving at the Targets step of the wizard] In the Choose monthly backup target section of the opened window, choose whether you want to store monthly backups in the archive repository.

   If you set the Send backups to archive toggle to On, follow the instructions provided in section Enabling Backup Archiving.

3. In the Create monthly schedule section, select months when the backup policy will create cloud-native snapshots, snapshot replicas or image-level backups.

   **NOTE**

   Veeam Backup for AWS does not create snapshot replicas and image-level backups independently from cloud-native snapshots. That is why when you select months to create snapshot replicas and image-level backups, the same months are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see EC2 Backup.

4. Use the Create restore point at and Run on drop-down lists to schedule a specific time and day for the backup policy to run.
NOTE
Consider the following:

- If you have selected a specific time for the backup policy to run at the **Weekly schedule** section of the **Schedule** step of the wizard, you will not be able to change the time for the monthly schedule unless you select the **On Day** option from the **Run on** drop-down list.
- If you select the **On day** option, **harmonized scheduling** cannot be guaranteed. Plus, to support the **On day** option, Veeam Backup for AWS will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed during the **Backup Retention** process from the AWS infrastructure in approximately 24 hours, to reduce unexpected infrastructure charges.

5. In the **Monthly retention** section, configure retention policy settings for the monthly schedule:
   - For cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.
     If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from each chain. For more information, see **EC2 and RDS Snapshot Retention**.
   - For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.
     If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see **EC2 Backup Retention**.

6. To save changes made to the backup policy settings, click **Apply**.
Specifying Yearly Schedule

[This step applies only if you have instructed Veeam Backup for AWS to create image-level backups at the Targets step of the wizard]

To create a yearly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Yearly schedule toggle to On and click Edit Yearly Settings.

2. [This step applies if you enabled backup archiving at the Targets step of the wizard] In the Choose yearly backup target section of the opened window, choose whether you want to store yearly backups in the archive repository.

   If you set the Send backups to archive toggle to On, follow the instructions provided in section Enabling Backup Archiving.

3. In the Yearly schedule section, specify a day, month and time when the backup policy will create image-level backups.

   For example, if you select First, Friday, January and 06:00 PM, the backup policy will run every first Friday of January at 06:00 PM.

   **NOTE**

   Consider the following:

   - If you have selected a specific time for the backup policy to run at the Weekly schedule or Monthly schedule sections of the Schedule step of the wizard, you will not be able to change the time for the yearly schedule unless you select the On Day option from the Create restore point on drop-down list.

   - If you select the On day option, harmonized scheduling cannot be guaranteed. Plus, to support the On day option, Veeam Backup for AWS will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed during the Backup Retention process from the AWS infrastructure in approximately 24 hours, to reduce unexpected infrastructure charges.

4. In the Keep backups for field, specify the number of years for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore from the chain. For more information, see EC2 Backup Retention.
5. To save changes made to the backup policy settings, click **Apply**.

### Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for AWS applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of retaining restore points.

With harmonized scheduling, Veeam Backup for AWS can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time:

- Cloud-native snapshots and snapshot replicas can be kept for weeks and months.
- Image-level backups can be kept for weeks, months and years.

For Veeam Backup for AWS to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of storing restore points. In terms of harmonized scheduling, Veeam Backup for AWS re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (D) flag is used to mark restore points created according to the daily schedule, (W) — weekly, (M) — monthly, and (Y) — yearly. Veeam Backup for AWS uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

**NOTE**

Restore points created according to a more-frequent schedule and less-frequent schedules compose a single backup or snapshot chain. This means that regardless of flags assigned to restore points, Veeam Backup for AWS adds the restore points to the chain as described in sections **Backup Chain** and **Snapshot Chain**.
Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to keep one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

- In the daily scheduling settings, you select hours and days when snapshots will be created (for example, **7:00 AM, 9:00 AM, and 11:00 AM, Working Days**), and specify a number of daily restore points to retain (for example, **3**).

Veeam Backup for AWS will propagate these settings to the schedule of a less-frequent schedule (which is the weekly schedule in our example).

- In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule will be retained for a longer period, and choose for how long you want to keep the selected snapshot.

For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select **7:00 AM, Monday** and specify 2 restore points to retain in the weekly schedule settings.
According to the specified scheduling settings, Veeam Backup for AWS will create cloud-native snapshots in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.  
   Since 7:00 AM, Monday is specified in weekly schedule settings, Veeam Backup for AWS will assign the (W) flag to this restore point as the weekly retention scheme is also applied to it.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (D) flag.

3. On the next work day (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   By the moment the backup session completes, the number of restore points with the (D) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for AWS will not remove the earliest restore point (7:00 AM, Monday) with the (D) flag from the snapshot chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for AWS will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (D) flag will exceed the retention limit once again. Veeam Backup for AWS will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a less-frequent schedule are assigned to this restore point.

5. Veeam Backup for AWS will continue creating restore points for the next week in the same way as described in steps 1–4.
6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of weekly restore points will exceed the retention limit. Veeam Backup for AWS will unassign the (W) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for AWS will remove this restore point from the snapshot chain.

Enabling Backup Archiving

When you combine multiple types of schedules, you can enable the archiving mechanism to instruct Veeam Backup for AWS to store backed-up data in the secure, low-cost and long-term S3 Glacier and S3 Glacier Deep Archive storage classes. The mechanism is the most useful in the following cases:

- Your data retention policy requires that you keep rarely accessed data in an archive.
- You want to reduce data-at-rest costs and to save space in the high-cost, short-term S3 standard storage class.

However, restoring from an archived backup is longer and more expensive than restoring from a standard backup as it is required to retrieve data from the archive repository. For more information, see Retrieving Data From Archive.

With backup archiving, Veeam Backup for AWS can retain backup files created according to a daily, weekly or monthly schedule for longer periods of time:

- To enable monthly archiving, you must configure a daily or a weekly schedule (or both).
- To enable yearly archiving, you must configure a daily, a weekly or a monthly schedule (or all three).

For Veeam Backup for AWS to use the archiving mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of backup files, while another schedule will control the process of copying backup files to an archive repository. Backup chains created according to these two schedules will be completely different — for more information, see EC2 Backup Chain and Archive Backup Chain.

Consider the following example. You want a backup policy to create image-level backups of your critical workloads once a week, to keep the backed-up data in a standard backup repository for 3 weeks, and also to keep backups created once in 2 months in an archive backup repository for a year. In this case, you create 2 schedules when configuring the backup policy settings — weekly and monthly:

1. In the policy target settings, you set the Enable backups toggle to On, select a backup repository that will store standard backup files, and select an archive repository that will store archived data.
2. In the weekly scheduling settings, you select hours and days when backups will be created (for example, 7:00 AM, Monday), and specify a number of days for which Veeam Backup for AWS will retain backups (for example, 21 days).

Veeam Backup for AWS will propagate these settings to the archive schedule (which is the monthly schedule in our example).

3. In the monthly scheduling settings, you enable the archiving mechanism by setting the Send backups to archive toggle to On, specify when Veeam Backup for AWS will create archive backup files, and choose for how long you want to keep the created backups in the archive repository.

For example, January, March, May, July, September, November, 12 months and First Monday.
IMPORTANT

Mind the following:

- When you enable backup archiving, you become no longer able to create a schedule of the same frequency for standard backups. By design, these two functionalities are mutually exclusive.
- If you enable backup archiving, it is recommended that you set the Snapshots to keep value to 0, to reduce unexpected snapshot charges.
- If you enable backup archiving, it is recommended that you set the Keep archives for value to at least 3 months (or 90 days) for S3 Glacier storage class and at least 6 months (or 180 days) for S3 Glacier Deep Archive storage class. For more information on minimum storage duration of the Amazon S3 archival storage classes, see AWS Documentation.
- If you select the On day option, harmonized scheduling cannot be guaranteed. Plus, to support the On day option, Veeam Backup for AWS will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed during the Backup Retention process from the AWS infrastructure in approximately 24 hours, to reduce unexpected infrastructure charges.

According to the specified scheduling settings, Veeam Backup for AWS will create image-level backups in the following way:

1. On the first Monday of February, a backup session will start at 7:00 AM to create the first restore point in the standard backup chain. Veeam Backup for AWS will store this restore point as a full backup file in the backup repository.
2. On the second and third Mondays of February, Veeam Backup for AWS will create restore points at 7:00 AM and add them to the standard backup chain as incremental backup files in the backup repository.

3. On the fourth Monday of February, Veeam Backup for AWS will create a new restore point at 7:00 AM. By the moment the backup session completes, the earliest restore point in the standard backup chain will get older than the specified retention limit. That is why Veeam Backup for AWS will rebuild the full backup file and remove from the chain the restore point created on the first Monday.

For more information on how Veeam Backup for AWS transforms standard backup chains, see EC2 Backup Retention.
4. On the first Monday of March, a backup session will start at 7:00 AM to create another restore point in the standard backup chain. At the same time, the earliest restore point in the standard backup chain will get older than the specified retention limit again. That is why Veeam Backup for AWS will rebuild the full backup file again and remove from the chain the restore point created on the second Monday.

After the backup session completes, an archive session will create a restore point with all data from the standard backup chain. Veeam Backup for AWS will copy this restore point as a full archive backup file to the archive repository.

5. Up to May, Veeam Backup for AWS will continue adding new restore points to the standard backup chain and deleting outdated backup files from the backup repository, according to the specified weekly scheduling settings.

On the first Monday of May, an archive session will create a restore point with only that data that has changed since the previous archive session in March. Veeam Backup for AWS will copy this restore point as an incremental archive backup file to the archive repository.
6. Up to the first Monday of February of the next year, Veeam Backup for AWS will continue adding new restore points to the standard backup chain and deleting outdated backup files from the backup repository, according to the specified weekly scheduling settings. Veeam Backup for AWS will also continue adding new restore points to the archive backup chain, according to the specified monthly settings.

By the moment the archive session completes, the earliest restore point in the archive backup chain will get older than the specified retention limit. That is why Veeam Backup for AWS will rebuild the full archive backup file and remove from the chain the restore point created on the first Monday of March of the previous year.

For more information on how Veeam Backup for AWS transforms archive backup chains, see Retention Policy for Archived Backups.
Step 7. Enable AWS Tags Assigning

At the Tags step of the wizard, you can instruct Veeam Backup for AWS to assign AWS tags to snapshots and snapshots replicas:

1. To assign already existing AWS tags from the EBS volumes of the processed EC2 instance, select the Copy tags from source volumes check box.

   If you choose to copy tags from source volumes, Veeam Backup for AWS will first create a cloud-native snapshot or snapshot replica of the EC2 instance and will assign to the created snapshot AWS tags with Veeam metadata, then Veeam Backup for AWS will copy tags from the volumes of the processed instance and, finally, assign the copied AWS tags to the snapshot.

2. To assign your own custom AWS tags, set the Add custom tags to created snapshots toggle to On and specify the AWS tags explicitly. To do that, use the Key and Value fields to specify a key and a value for the new custom AWS tag, and then click Add. Note that you cannot add more than 5 custom AWS tags.

   If you choose to add custom tags to created snapshots, Veeam Backup for AWS will assign the specified tags right after it creates a cloud-native snapshot or snapshot replica.
Step 8. Specify General Settings

At the **General Settings** step of the wizard, you can enable automatic retries, schedule health checks and specify notification settings for the backup policy.

### Automatic Retry Settings

To instruct Veeam Backup for AWS to run the backup policy again if it fails on the first try, do the following:

1. In the **Schedule** section of the step, select the **Automatic retry failed policy** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 60 seconds.

When retrying backup policies, Veeam Backup for AWS processes only those instances that failed to be backed up during the previous attempt.

### Health Check Settings

If you have enabled creation of image-level backups at **step 5** of the wizard, you can instruct Veeam Backup for AWS to periodically perform a health check for backup restore points created by the policy. During the health check, Veeam Backup for AWS performs an availability check for data blocks in the whole standard backup chain, and a cyclic redundancy check (CRC) for storage metadata to verify its integrity. The health check helps you ensure that the restore points are consistent and that you will be able to restore data using these restore points. For more information on the health check, see [How Health Check Works](#).

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>During a health check, Veeam Backup for AWS does not verify archived restore points created by the policy.</td>
</tr>
</tbody>
</table>

To enable monthly health checks for the backup policy, do the following:

1. In the **Health check** section of the step, set the **Enable health check** toggle to *On*.
2. Use the **Run on** drop-down lists to schedule a specific day for the health check to run.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup for AWS performs the health check during the first policy session that runs on the day when the health check is scheduled. If another backup policy session runs on the same day, Veeam Backup for AWS will not perform the health check during that session. For example, if the backup policy is scheduled to run multiple times on Saturday, and the health check is also scheduled to run on Saturday, the health check will only be performed during the first policy session on Saturday.</td>
</tr>
</tbody>
</table>

### Email Notification Settings

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>To be able to specify email notification settings for the EC2 Backup policy, you must configure the SMTP server settings first. For more information on how to configure the SMTP server settings, see Configuring Global Email Notification Settings.</td>
</tr>
</tbody>
</table>

233 | Veeam Backup for AWS | User Guide
To instruct Veeam Backup for AWS to send email notifications for the backup policy, do the following:

1. In the **Notifications** section of the step, set the **Enabled** toggle to **On**.
   
   If you set the toggle to **Off**, Veeam Backup for AWS will send notifications according to the configured **global notification settings**.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.

3. Use the **Notify on** list to choose whether you want Veeam Backup for AWS to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

4. Select the **Suppress notifications until the last retry** check box to receive a notification about the final backup policy result.
   
   If you do not select the check box, Veeam Backup for AWS send a notification for every backup policy retry.

**NOTE**

If you specify the same email recipient in both backup policy notification and **global notification settings**, Veeam Backup for AWS will override the configured **global notification settings** and will send each notification to this recipient only once to avoid notification duplicates.
How Health Check Works

When Veeam Backup for AWS saves a new backup restore point to a backup repository, it calculates CRC values for metadata in the backup chain and saves these values to the chain metadata, together with the instance data. When performing a health check, Veeam Backup for AWS verifies the availability of data blocks and uses the saved values to ensure that the restore points being verified are consistent.

If you have enabled monthly health checks for the backup policy, Veeam Backup for AWS performs the following operations at the day scheduled for a health check to run:

1. As soon as a backup policy session completes successfully, Veeam Backup for AWS starts the health check as a new session. For each restore point in the standard backup chain, Veeam Backup for AWS calculates CRC values for backup metadata and compares them to the CRC values that were previously saved to the restore point. Veeam Backup for AWS also checks whether data blocks that are required to rebuild the restore point are available.

   If the backup policy session completes with an error, Veeam Backup for AWS tries to run the backup policy again, taking into account the maximum number of retries specified in the automatic retry settings. After the first successful retry (or after the last one out of the maximum number of retries), Veeam Backup for AWS starts the health check.

2. If Veeam Backup for AWS does not detect data inconsistency, the health check session completes successfully. Otherwise, the session completes with an error.

   Depending on the detected data inconsistency, Veeam Backup for AWS performs the following operations:

   - If the health check detects corrupted metadata in a full or incremental restore point, Veeam Backup for AWS marks the backup chain as corrupted in the configuration database. During the next backup policy session, Veeam Backup for AWS copies the full instance image, creates a full restore point in the backup repository and starts a new backup chain in the backup repository.

   **NOTE**

   Veeam Backup for AWS does not support metadata check for encrypted backup chains.

   - If the health check detects corrupted disk blocks in a full or an incremental restore point, Veeam Backup for AWS marks the restore point that includes the corrupted data blocks and all subsequent incremental restore points as incomplete in the configuration database. During the next backup policy session, Veeam Backup for AWS copies not only those data blocks that have changed since the previous backup session but also data blocks that have been corrupted, and saves these data blocks to the latest restore point that has been created during the current session.
Step 9. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the **Schedule** step of the wizard]

At the **Cost Estimation** step of the wizard, review the estimated monthly cost of AWS services and resources that will be consumed to protect the instances added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining cloud-native snapshots of the instances.
  
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance type, the number of EBS volumes attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating snapshot replicas and maintaining them in the target AWS Region.
  
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance type, the number of EBS volumes attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating and storing in backup repositories image-level backups of the instances.
  
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance type, the number of EBS volumes attached, the number of restore points to be kept in the backup chain, and the configured scheduling settings.

- The cost of creating and storing in archive repositories archived backups of the instances.
  
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the machine type, the number of EBS volumes attached, the number of restore points to be kept in the backup chain, and the configured scheduling settings.

- The cost of transferring the instance data between AWS Regions during data protection operations (for example, if a protected instance and the target backup repository reside in different regions).
  
  If you get a warning message regarding additional costs associated with cross-region data transfer, you can click **View details** to see available cost-effective options.

- The cost of sending API requests to Veeam Backup for AWS during data protection operations.

To calculate the estimated cost, Veeam Backup for AWS uses capabilities of the [Amazon Web Services Simple Monthly Calculator](https://calculator.aws). The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can try the following workarounds:

- To avoid additional costs related to cross-region data transfer, select a backup repository that resides in the same region as instances that you plan to back up.

- To reduce high snapshot charges, adjust the snapshot retention settings to keep less restore points in the snapshot chain.

- To optimize the cost of storing backups, configure the scheduling settings to run the backup policy less frequently, or specify an archive repository for long-term retention of restore points.

For more information on cost estimation, see [this Veeam KB article](https://kb.veeam.com).
TIP

You can save the cost estimation as a .CSV or .XML file. To do that, click Export to and select the necessary format.

Related Resources

How AWS Pricing Works
Step 10. Finish Working with Wizard

At the Summary step of the wizard, it is recommended that you run the backup policy configuration check before you click Finish.

The configuration check will verify whether specified IAM roles have all the required permissions, and networks settings are configured properly to launch worker instances. To run the check, click Test Configuration. Veeam Backup for AWS will display the Test policy configuration window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient or policy settings are not configured properly, the check will complete with errors, and the list of permissions that must be granted to the IAM role and policy configuration issues will be displayed in the Test policy configuration window.

You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Test policy configuration window, click the Grant link.
2. In the Grant Permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

The IAM user must have the following permissions:

```
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"
```

NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. After the required permissions are granted, close the **Test policy configuration** window, and then click **Finish** to close the **Add Policy** wizard.

Veeam Backup for AWS will save the configured backup policy.

Fixing Network Issues

If the backup policy check reveals that network settings are not configured properly, Veeam Backup for AWS will not be able to launch worker instances and thus perform image-level backup.

To fix network issues:

1. Close the **Test policy configuration** window, and then click **Finish** to close the **Add Policy** wizard.

Veeam Backup for AWS will save the configured backup policy.

2. To prevent the backup policy from failing, disable it. For details, see Disabling and Enabling Backup Policies.

3. Depending on the error message received after the backup policy check, do the following:
   
   - Make sure that network settings are configured for each AWS Region selected at step 3.2. For information on how to configure network settings for AWS Regions, see Managing Worker Configurations.
   
   - Make sure that VPCs specified in network settings for AWS Regions have access to the required AWS services. The required AWS services are listed in the System Requirements section.

4. After network issues are fixed, you can enable the backup policy. For details, see Disabling and Enabling Backup Policies.
Creating EC2 Snapshots Manually

Veeam Backup for AWS allows you to manually create snapshots of EC2 instances. You can instruct Veeam Backup for AWS to store the created snapshots in the same AWS Regions where the processed EC2 instances reside, or in a different AWS Region or AWS account.

NOTE

Veeam Backup for AWS does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your AWS environment unless you remove them manually, as described in section Managing Backed-Up EC2 Instance Data.

To manually create a cloud-native snapshot of an EC2 instance, do the following:

1. Navigate to Resources > EC2.
2. Select the necessary instance and click **Take Snapshot Now**.

   For an EC2 instance to be displayed in the list of available instances, an AWS Region where the instance resides must be added to any of configured EC2 backup policies, and the IAM role specified in the backup policy settings must have permissions to access the instance. For more information on required permissions, see EC2 Backup IAM Role Permissions.

3. Complete the **Take Manual Snapshot** wizard:

   a. At the **Account** step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to create the snapshot.

      For an IAM role to be displayed in the list, it must be added to Veeam Backup for AWS as described in section Adding IAM Roles.

   b. At the **Snapshot Mode** step of the wizard, choose whether you want to store the snapshot in the same AWS Region where the processed EC2 instance resides, or in another AWS Region or AWS account.

   c. [Applies if you have selected the New location option] At the **Settings** step of the wizard, choose an IAM role whose permissions will be used to copy and store the snapshot in a target AWS Region, the target AWS Region and specify whether to encrypt the copied snapshot.

   d. At the **Tags** step of the wizard, choose whether you want to assign AWS tags to the created snapshot.

      - To assign already existing AWS tags from the EBS volumes of the processed EC2 instance, select the **Copy tags from source volumes** check box.

      If you choose to copy tags from source volumes, Veeam Backup for AWS will first create a snapshot of the EC2 instance and assign to the created snapshot AWS tags with Veeam metadata, then Veeam Backup for AWS will copy tags from the volumes of the processed instance and, finally, assign the copied AWS tags to the snapshot.

      - To assign your own custom AWS tags, click **Add** and specify the tags explicitly. To do that, in the **Add Custom Tag** window, specify a key and a value for the new AWS tag, and then click **Apply**. Note that you cannot add more than 5 custom AWS tags.

      If you choose to add custom tags to created snapshots, Veeam Backup for AWS will assign the specified tags right after it creates a snapshot.
e. At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing RDS Backup

To produce cloud-native snapshots and snapshot replicas of DB instances and Aurora DB clusters, Veeam Backup for AWS runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where backups must be stored, when the backup process must start and so on.

You can create multiple RDS backup policies. One backup policy can be used to process multiple DB instances and Aurora DB clusters within different AWS Regions, but you can protect each RDS resource with one backup policy at a time. If an RDS resource is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this RDS resource from processing. For information on how to set a priority for a backup policy, see Setting Policy Priority.

For DB instances and Aurora DB clusters residing in any of the regions added to the backup policies, you can also take a cloud-native snapshot manually when needed.
Creating RDS Backup Policies

One backup policy can be used to process one or more RDS resources within one AWS account. The scope of data that you can protect in an AWS account is limited by permissions of an IAM role that is specified in the backup policy settings.

**NOTE**
Before you create an RDS backup policy, if you plan to receive email notifications on backup policy results, configure SMTP server settings first. For more information, see Configuring Global Email Notification Settings.

To create an RDS backup policy, complete the following steps:

1. Launch the Add RDS Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Configure backup target settings.
5. Specify a schedule for the backup policy.
7. Review estimated cost for protecting RDS resources.
8. Finish working with the wizard.
Step 1. Launch Add RDS Policy Wizard

To launch the Add RDS Policy wizard, complete the following steps.

1. Navigate to Policies > RDS.
2. Click Add.
Step 2. Specify Policy Name and Description

At the **Info** step of the wizard, use the **Name** and **Description** fields to specify a name for the new backup policy and to provide a description for future reference. The name must be unique in Veeam Backup for AWS; the maximum length of the name is 127 characters, the maximum length of the description is 255 characters.
Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify backup source settings:

1. **Select an IAM role whose permissions will be used to perform RDS backup.**
2. **Select AWS Regions where RDS resources that you plan to back up reside.**
3. **Select DB instances and Aurora DB clusters to back up.**
Step 3.1 Specify IAM Role

In the IAM role section of the Sources step of the wizard, you must specify an IAM role whose permissions will be used to access AWS services and resources, and to create cloud-native snapshots of DB instances and Aurora DB clusters. If you specify an IAM role created in another AWS account, the backup policy will process RDS resources on which the specified IAM role has permissions in that AWS account.

For an IAM role to be displayed in the IAM role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the Add Policy wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

TIP

To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click Export Missing Permissions.

IMPORTANT

If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Permission check window, click Grant.

2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

   The IAM user must have the following permissions:

```
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"
```

NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. To make sure that the missing permissions have been successfully granted, click **Recheck**.
Step 3.2 Select AWS Regions

In the **Regions** section of the **Sources** step of the wizard, choose AWS Regions where RDS resources that you plan to back up reside.

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions, click **Add** to include them in the backup policy.
3. To save changes made to the backup policy settings, click **Apply**.
Step 3.3 Select RDS Resources

In the Resources section of the Sources step of the wizard, specify the backup scope — select DB instances and Aurora DB clusters that Veeam Backup for AWS will back up:

1. Click Choose resources to protect.

2. In the Choose resources to protect window, choose whether you want to back up all RDS resources from AWS Regions selected at step 3, or only specific RDS resources.

   If you select the All resources option, Veeam Backup for AWS will regularly check for new DB instances and Aurora DB clusters launched in the selected regions and automatically update the backup policy settings to include these resources in the backup scope.

   If you select the Protect only following resources option, you must also specify the resources explicitly:

   a. Use the Resource type drop-down list to choose whether you want to add individual RDS resources or AWS tags to the backup scope.

      If you select the Tag option, Veeam Backup for AWS will back up only those resources from the selected AWS Regions that are assigned specific tags.

   b. Use the search field to the right of the Resource type list to find the necessary resource, and then click Protect to add the resource to the backup scope.

      For a resource to be displayed in the list of available resources, it must reside in an AWS Region that has ever been specified in any backup policy. Otherwise, the only option to discover the available resources is to click Browse to select specific resources from the global list and to wait for Veeam Backup for AWS to populate the resource list.

      TIP

      You can simultaneously add multiple resources to the backup scope. To do that, click Browse to select specific sources from the global list, select check boxes next to the necessary RDS resources or AWS tags in the list of available resources, and then click Protect.

      If the list does not show the resources that you want to back up, click Rescan to launch the data collection process. As soon as the process is over, Veeam Backup for AWS will update the resource list.

      If you add an AWS tag to the backup scope, Veeam Backup for AWS will regularly check for new RDS resources assigned the added AWS tag and automatically update the backup policy settings to include these resources in the scope. However, this applies only to DB instances and Aurora DB clusters from the AWS Regions selected at step 3. If you select an AWS tag assigned to RDS resources from other AWS Regions, these resources will not be protected by the backup policy. To work around the issue, either go back to step 3 and add the missing AWS Regions, or create a new backup policy.
3. To save changes made to the backup policy settings, click **Apply**.
Step 4. Configure Backup Target Settings

By default, backup policies create only cloud-native snapshots of processed instances. At the Targets step of the wizard, you can enable the following additional data protection scenarios:

- Instruct Veeam Backup for AWS to replicate cloud-native snapshots to other AWS accounts or AWS Regions.

- Assign AWS tags to created cloud-native snapshots.

Configuring Snapshot Replica Settings

If you want to replicate cloud-native snapshots to other AWS accounts or regions, do the following:

1. In the Snapshots section of the Targets step of the wizard, set the Replicate snapshots toggle to On.

2. In the Replication settings window, configure the following mapping settings for each AWS Region where source instances reside:

   **IMPORTANT**

   Mind that several limitations are applied to Aurora DB clusters:

   - Snapshot replication is not supported for Aurora multi-master clusters.
   - Snapshot replication is not supported for the following regions: Africa (Cape Town), Asia Pacific (Hong Kong), Europe (Milan), Middle East (Bahrain). For more information, see AWS Documentation.
   - If DB engine versions of the processed Aurora DB clusters are not supported in the target AWS Region, the replication operation will fail. For the list of supported DB engine versions in AWS Regions, see AWS Documentation.

   a. Select a source AWS Region in the list and click Edit Region Mapping.

   b. In the Edit Region Mapping window, specify the following settings:

      i. From the Target account drop-down list, select an IAM role whose permissions will be used to copy and store cloud-native snapshots in a target AWS Region.

         If you select an IAM role created in another AWS account, the cloud-native snapshot will be copied to the target AWS Region in that AWS account.

      ii. From the Target region drop-down list, select the target AWS Region to which Veeam Backup for AWS must copy cloud-native snapshots.

      iii. If you want to encrypt cloud-native snapshots copied to the target AWS Region, select the Enable encryption check box and choose the necessary KMS key from the Encryption key drop-down list. For a KMS key to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 3 and the IAM role specified for the backup operation must have permissions to the key. For more information on KMS keys, see AWS Documentation.

         Then use the Key usage drop-down list to choose whether you want to encrypt snapshots for all resources or only snapshots of the encrypted resources.
NOTE
Consider the following:

- If the source DB instances or Aurora DB cluster is encrypted, you must enable encryption for replicated snapshots, otherwise the replication process will fail.

- If the source Aurora DB cluster is unencrypted, you must not enable encryption for replicated snapshots, otherwise the replication process will fail.

div. Click **Save**.

To configure mapping for all source AWS Regions at once, click **Set Mapping for All Regions** and specify settings as described in step 2.b.

c. To save changes made to the backup policy settings, click **Apply**.

Enabling AWS Tags Assigning

In the **Tags** section of the **Targets** step of the wizard, choose whether you want to assign AWS tags to snapshots and snapshots replicas. To assign AWS tags, click **Edit Tag Settings**.

In the **Tag configuration** window, specify tag settings:

1. To assign already existing AWS tags from the processed RDS resources, select the **Copy tags from source RDS instances** check box.

   If you choose to copy tags from source instances, Veeam Backup for AWS will first create a cloud-native snapshot or snapshot replica of the DB instance or Aurora DB cluster and assign to the created snapshot AWS tags with Veeam metadata, then Veeam Backup for AWS will copy tags from the processed instance and finally assign the copied AWS tags to the snapshot.
2. To assign your own custom AWS tags, set the **Add custom tags to created snapshots** toggle to **On** and specify the AWS tags explicitly. To do that, use the **Key** and **Value** fields to specify a key and a value for the new custom AWS tag, and then click **Add**. Note that you cannot add more than 5 custom AWS tags.

   If you choose to add custom tags to created snapshots, Veeam Backup for AWS will assign the specified tags right after it creates a cloud-native snapshot or snapshot replica.

3. To save changes made to the backup policy settings, click **Apply**.
Step 5. Specify Policy Scheduling Options

You can instruct Veeam Backup for AWS to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the instances added to the backup policy must be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for AWS allows you to create schedules of the following types:

- **Daily** — the backup policy will create restore points repeatedly throughout a day on specific days.
- **Weekly** — the backup policy will create restore points once a day on specific days.
- **Monthly** — the backup policy will create restore points once a month on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time. For more information, see Enabling Harmonized Scheduling.

**NOTE**

If you do not specify the backup schedule, after you configure the backup policy, you will need to start it manually to create RDS backups. For information on how to start backup policies, see Starting and Stopping Policies.

Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily schedule** toggle to **On** and click **Edit Daily Settings**.
2. In the **Create daily schedule** window, select hours when the backup policy must create cloud-native snapshots and snapshot replicas.
   
   If you want to protect RDS resources data more frequently, you can instruct the backup policy to create multiple cloud-native snapshots per hour. To do that, click the link to the right of the **Snapshots** hour selection area, and specify the number of cloud-native snapshots that the backup policy must create within an hour.

   **NOTE**

   Veeam Backup for AWS does not create snapshot replicas independently from cloud-native snapshots. That is why when you select hours to create snapshot replicas, the same hours are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see RDS Backup.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on work days (Monday through Friday) or on specific days.

4. In the **Daily retention** section, for cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.
   
   If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see EC2 and RDS Snapshot Retention.
5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly schedule** toggle to **On** and click **Edit Weekly Settings**.
2. In the **Create weekly schedule** window, select weekdays when the backup policy must create cloud-native snapshots and snapshot replicas.

**NOTE**

Mind that Veeam Backup for AWS does not create snapshot replicas independently from cloud-native snapshots. That is why when you select days to create snapshot replicas, the same days are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see [RDS Backup](#).

3. Use the **Create restore point at** drop-down list to schedule a specific time for the backup policy to run.
4. In the **Weekly retention** section, for cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains.
   
   If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see [EC2 and RDS Snapshot Retention](#).
5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Monthly schedule** toggle to **On** and click **Edit Monthly Settings**.
2. In the **Create monthly schedule** window, select months when the backup policy must create cloud-native snapshots and snapshot replicas.

**NOTE**

Mind that Veeam Backup for AWS does not create snapshot replicas independently from cloud-native snapshots. That is why when you select months to create snapshot replicas, the same months are automatically selected for cloud-native snapshots. To learn how Veeam Backup for AWS performs backup, see **RDS Backup**.

3. Use the **Create restore point at** and **Run on** drop-down lists to schedule a specific time and day for the backup policy to run.

**NOTE**

Consider the following:

- If you have selected a specific time for the backup policy to run at the **Weekly schedule** section of the **Schedule** step of the wizard, you will not be able to change the time for the monthly schedule unless you select the **On Day** option from the **Run on** drop-down list.
- If you select the **On day** option, **harmonized scheduling** cannot be guaranteed. Plus, to support the **On day** option, Veeam Backup for AWS will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed by the **Backup Retention** process from the AWS infrastructure during approximately 24 hours, to reduce unexpected infrastructure charges.
4. In the **Monthly retention** section, for cloud-native snapshots and snapshot replicas, specify the number of restore points that you want to keep in cloud-native snapshot and snapshot replica chains. If the restore point limit is exceeded, Veeam Backup for AWS removes the earliest restore point from the chain. For more information, see [EC2 and RDS Snapshot Retention](#).

5. To save changes made to the backup policy settings, click **Apply**.

---

**Enabling Harmonized Scheduling**

When you combine multiple types of schedules, Veeam Backup for AWS applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of retaining restore points.

With harmonized scheduling, Veeam Backup for AWS can keep restore points created according to a daily or weekly schedule for longer periods of time: cloud-native snapshots and snapshot replicas can be kept for weeks and months.

For Veeam Backup for AWS to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of storing restore points. In terms of harmonized scheduling, Veeam Backup for AWS re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (D) flag is used to mark restore points created daily, (W) — weekly, (M) — monthly, and (Y) — yearly. Veeam Backup for AWS uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.
Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to keep one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

- In the daily scheduling settings, you select hours and days when snapshots must be created (for example, 7:00 AM, 9:00 AM, and 11:00 AM, Working Days), and specify a number of daily restore points to retain (for example, 3). Veeam Backup for AWS will propagate these settings to the schedule of a less-frequent schedule (which is the weekly schedule in our example).

- In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule must be retained for a longer period, and choose for how long you want to keep the selected snapshot. For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select 7:00 AM, Monday and specify 2 restore points to retain in the weekly schedule settings.
According to the specified scheduling settings, Veeam Backup for AWS will create cloud-native snapshots in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.

   Since 7:00 AM, Monday is specified in weekly schedule settings, Veeam Backup for AWS will assign the (W) flag to this restore point.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (D) flag.

3. On the next work day (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

   By the moment the backup session completes, the number of restore points with the (D) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for AWS will not remove the earliest restore point (7:00 AM, Monday) with the (D) flag from the snapshot chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for AWS will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (D) flag will exceed the retention limit once again. Veeam Backup for AWS will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a less-frequent schedule are assigned to this restore point.

5. Veeam Backup for AWS will continue creating restore points for the next week in the same way as described in steps 1–4.
6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of weekly restore points will exceed the retention limit. Veeam Backup for AWS will unassign the (W) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for AWS will remove this restore point from the snapshot chain.
Step 6. Specify Retry and Email Notification Settings

At the General Settings step of the wizard, you can enable automatic retries and specify notification settings for the backup policy.

Automatic Retry Settings

To instruct Veeam Backup for AWS to run the backup policy again if it fails on the first try, do the following:

1. In the Schedule section of the step, select the Automatically retry failed policy check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 60 seconds.

When retrying backup policies, Veeam Backup for AWS processes only those instances that failed to be backed up during the previous attempt.

Email Notification Settings

NOTE

To be able to specify email notification settings for the RDS Backup policy, you must configure the SMTP server settings first. For more information on how to configure the SMTP server settings, see Configuring Global Email Notification Settings.

To instruct Veeam Backup for AWS to send email notifications for the backup policy, do the following:

1. In the Notifications section of the step, set the Enabled toggle to On.

   If you set the toggle to Off, Veeam Backup for AWS will send notifications according to the configured global notification settings.

2. In the Email field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.

3. Use the Notify on list to choose whether you want Veeam Backup for AWS to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

4. Select the Suppress notifications until the last retry check box to receive a notification about the final backup policy result.

   If you do not select the check box, Veeam Backup for AWS send a notification for every backup policy retry.
NOTE

If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for AWS will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.
Step 7. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the Schedule step of the wizard]

At the Cost Estimation step of the wizard, review the estimated monthly cost of AWS services and resources that will be consumed to protect the instances added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining cloud-native snapshots of the instances.
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance class, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating snapshot replicas and maintaining them in the target AWS Region.
  For each instance included in the backup policy, Veeam Backup for AWS takes into account the instance class, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of sending API requests to Veeam Backup for AWS during data protection operations.

To calculate the estimated cost, Veeam Backup for AWS uses capabilities of the Amazon Web Services Simple Monthly Calculator.

The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can adjust the snapshot retention settings to keep less restore points in the snapshot chain.

TIP

You can save the cost estimation as a .CSV or .XML file. To do that, click Export to and select the necessary format.
Related Resources

How AWS Pricing Works
Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, it is recommended that you run the backup policy configuration check before you click **Finish**.

The configuration check will verify whether specified IAM roles have all the required permissions. To run the check, click **Test Configuration**. Veeam Backup for AWS will display the **Test policy configuration** window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient or policy settings are not configured properly, the check will complete with errors. You can grant the missing permissions to the IAM role as described in section [Checking IAM Role Permissions](#).

After the required permissions are granted, close the **Test policy configuration** window, and then click **Finish** to close the **Add Policy** wizard.

Veeam Backup for AWS will save the configured backup policy.
Creating RDS Snapshots Manually

Veeam Backup for AWS allows you to manually create snapshots of RDS resources. You can instruct Veeam Backup for AWS to store the created snapshots in the same AWS Regions where the processed DB instances and DB clusters reside, or in a different AWS Region or AWS account.

**NOTE**

Veeam Backup for AWS does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your AWS environment unless you remove them manually, as described in section Managing Backed-Up RDS Data.

To manually create a cloud-native snapshot of a DB instance or Aurora DB cluster, do the following:

1. Navigate to Resources > RDS.
2. Select the necessary instance and click **Take Snapshot Now**.
   
   For an RDS resource to be displayed in the list of available instances, an AWS Region where the instance resides must be added to any of configured RDS backup policies, and the IAM role specified in the backup policy settings must have permissions to access the instance. For more information on required permissions, see [RDS Backup IAM Role Permissions](#).
3. Complete the **Take Manual Snapshot** wizard:
   
   a. At the **Account** step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to create the snapshot.
      
      For an IAM role to be displayed in the list, it must be added to Veeam Backup for AWS as described in section [Adding IAM Roles](#).
   
   b. At the **Snapshot Mode** step of the wizard, choose whether you want to store the snapshot in the same AWS Region where the processed RDS resource resides, or in another AWS Region or AWS account.
   
   c. [Applies if you have selected the **New location** option] At the **Settings** step of the wizard, choose an IAM role whose permissions will be used to copy and store the snapshot in a target AWS Region, the target AWS Region and specify whether to encrypt the copied snapshot.
   
   d. At the **Tags** step of the wizard, choose whether you want to assign AWS tags to the created snapshot.
      
      ▪ To assign already existing AWS tags from the source DB instance and Aurora DB cluster, select the **Copy tags from source RDS instance** check box.
         
         If you choose to copy tags from source RDS resource, Veeam Backup for AWS will first create a snapshot of the DB instance or Aurora DB cluster and assign to the created snapshot AWS tags with Veeam metadata, then Veeam Backup for AWS will copy tags from the processed resource and, finally, assign the copied AWS tags to the snapshot.
      
      ▪ To assign your own custom AWS tags, click **Add** and specify the tags explicitly. To do that, in the **Add Custom Tag** window, specify a key and a value for the new AWS tag, and then click **Apply**. Note that you cannot add more than 5 custom AWS tags.
         
         If you choose to add custom tags to created snapshots, Veeam Backup for AWS will assign the specified tags right after it creates a snapshot.
e. At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing EFS Backup

To back up Amazon EFS file systems, Veeam Backup for AWS runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where backups must be stored, when the backup process must start and so on.

One backup policy can be used to process multiple EFS file systems within different regions, but you can back up each file system with one backup policy at a time. If an EFS file system is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this file system from processing. For information on how to set a priority for a backup policy, see Setting Policy Priority.

For EFS systems residing in any of the regions added to the backup policies, you can also take a backup manually when needed.

**IMPORTANT**

You can back up EFS file systems only to the same AWS accounts where the source file systems belong.
Creating EFS Backup Policies

One backup policy can be used to process one or more EFS file systems within one AWS account. The scope of data that you can protect in an AWS account is limited by permissions of an IAM role that is specified in the backup policy settings.

**NOTE**

Before you create an EFS backup policy, if you plan to receive email notifications on backup policy results, configure SMTP server settings first. For more information, see [Configuring Global Email Notification Settings](#).

To create an EFS backup policy, complete the following steps:

1. **Launch the Add EFS Policy wizard.**
2. **Specify a backup policy name and description.**
3. **Configure backup source settings.**
4. **Enable indexing for the processed file systems.**
5. **Configure backup target settings.**
6. **Specify a schedule for the backup policy.**
7. **Enable AWS tags assigning.**
8. **Specify automatic retry settings and notification settings.**
9. **Review estimated cost for protecting EFS file systems.**
10. **Finish working with the wizard.**
Step 1. Launch Add EFS Policy Wizard

To launch the Add EFS Policy wizard, complete the following steps.

1. Navigate to Policies > EFS.
2. Click Add.
Step 2. Specify Policy Name and Description

At the **Info** step of the wizard, use the **Name** and **Description** fields to specify a name for the new backup policy and to provide a description for future reference. The name must be unique in Veeam Backup for AWS; the maximum length of the name is 127 characters, the maximum length of the description is 255 characters.
Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify backup source settings:

1. **Select an IAM role whose permissions will be used to perform EFS file system backup.**
2. **Select AWS Regions where EFS file systems that you plan to back up reside.**
3. **Select EFS file systems to back up.**
Step 3.1 Specify IAM Role

In the IAM role section of the Sources step of the wizard, you must specify an IAM role whose permissions will be used to access AWS services and resources, and to create backups of Amazon EFS file systems. If you specify an IAM role created in another AWS account, the backup policy will process EFS file systems on which the specified IAM role has permissions in that AWS account.

For an IAM role to be displayed in the IAM role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the Add Policy wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

**TIP**

To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click Export Missing Permissions.

**IMPORTANT**

If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Permission check window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

   The IAM user must have the following permissions:

   ```json
   "iam:CreatePolicy",
   "iam:GetRole",
   "iam:GetPolicy",
   "iam:AttachRolePolicy"
   ```

   **NOTE**

   Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. To make sure that the missing permissions have been successfully granted, click **Recheck**.
Step 3.2 Select AWS Regions

In the **Regions** section of the **Sources** step of the wizard, select AWS Regions where EFS file systems that you plan to back up reside.

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary AWS Regions from the **Available Regions** list, and click **Add**.
3. To save changes made to the backup policy settings, click **Apply**.
Step 3.3 Select EFS File Systems

In the Resources section of the Sources step of the wizard, specify the backup scope — select EFS file systems that Veeam Backup for AWS will back up:

1. Click Choose resources to protect.

2. In the Choose resources to protect window, choose whether you want to back up all EFS file systems from AWS Regions selected at step 3.2, or only specific file systems.

   If you select the All resources option, Veeam Backup for AWS will regularly check for new EFS file systems reside in the selected regions and automatically update the backup policy settings to include these file systems in the backup scope.

   If you select the Protect only following resources option, you must specify the EFS file systems explicitly:

   a. Use the Resource type drop-down list to choose whether you want to add individual file systems or AWS tags to the backup scope.

      If you select the Tag option, Veeam Backup for AWS will back up only those file systems that reside in the selected AWS Regions under specific AWS tags.

   b. Use the search field of the Name or ID list to find the necessary resource, and then click Protect to add the resource to the backup scope.

      Alternatively, you can click Browse to select specific sources from the global list, select check boxes next to the necessary file systems or AWS tags in the list of available resources, and then click Protect.

NOTE

By default, Veeam Backup for AWS uses an AWS CloudTrail trail to track changes in your EFS resources. If no trails are configured in the source AWS account, Veeam Backup for AWS will automatically access AWS resources and populate the list of available file systems or AWS tags only once in 24 hours. To manually force the data collection process, click Rescan.

If you add an AWS tag to the backup scope, Veeam Backup for AWS will regularly check for new Amazon EFS file systems assigned the added AWS tag and automatically update the backup policy settings to include these file systems in the scope. However, this applies only to file systems from the AWS Regions selected at step 3.2. If you select a tag assigned to file systems from other regions, these file systems will not be protected by the backup policy. To work around the issue, either go back to step 3.2 and add the missing regions, or create a new backup policy.
4. To save changes made to the backup policy settings, click **Apply**.
Step 4. Enable EFS Indexing

At the Indexing step of the wizard, you can instruct Veeam Backup for AWS to perform indexing of the processed EFS file systems. EFS indexing allows you to perform EFS file-level recovery operations without specifying the exact paths to the necessary files and to restore files using different restore points during one restore session. While performing EFS indexing of a file system, Veeam Backup for AWS creates a catalog of all files and directories (an index) and saves the index to a backup repository. This index is further used to reproduce the file system structure and to enable browsing and searching for specific files within an EFS backup.

To learn how indexing works, see EFS Backup.

NOTE

To perform indexing of the EFS file systems, Veeam Backup for AWS launches a worker instance per each processed file system in the same AWS account where the file system resides — production account. By default, the most appropriate network settings of AWS Regions are used to launch these worker instances. However, you can add specific worker configurations that will be used to launch worker instances used for EFS indexing operations.

Limitations and Requirements

Before you enable EFS indexing, consider the following:

- EFS indexing is not supported in the Free edition of Veeam Backup for AWS. For more information on license editions, see Licensing.

- Each processed EFS file system for which you want to perform indexing must meet the following requirements:
  - A file system must have at least one mount target created.
  - A mount target that will be used by worker instances to connect to the file system must be associated with a security group that allows inbound access on 2049 port.

- If no specific worker configurations are added to Veeam Backup for AWS, the most appropriate network settings of AWS Regions are used to launch worker instances for EFS indexing operation. For Veeam Backup for AWS to be able to launch a worker instance used to create an index of a file system:
  - A VPC in which the file system has the mount target must have at least one security group that allows outbound access on 2049 and 443 ports. These ports are used by worker instances to mount the file system and to communicate with AWS services.
  - The DNS resolution option must be enabled for the VPC. For more information, see AWS Documentation.
  - As Veeam Backup for AWS uses public access to communicate with worker instances, the public IPv4 addressing attribute must be enabled at least for one subnet in the Availability Zone in which the file system has a mount target and the VPC to which the subnet belong must have an internet gateway attached. VPC and subnet route tables must have routes that direct internet-bound traffic to this internet gateway.

If you want worker instances to operate in the private network, configure private endpoints for it to let Veeam Backup for AWS use private IPv4 addresses. To learn how to configure endpoints, see Appendix C. Configuring Endpoints in AWS.
Enabling EFS Indexing

To enable indexing of the processed file systems, do the following:

1. Set the **Enable Indexing** toggle to **On**.

2. In the **Repositories** window, select a repository where the created EFS indexes will be stored, and click **Apply**.

   For a backup repository to be displayed in the repository list, it must be added to Veeam Backup for AWS as described in section **Adding Backup Repositories**. The list shows only backup repositories of the **S3 Standard** storage class that have encryption enabled.

3. In the **IAM role** section, choose an IAM role that will be attached to worker instances launched to perform EFS indexing operations. Permissions of this role Veeam Backup for AWS will use to communicate with worker instances.

   For an IAM role to be displayed in the list, it must be added to Veeam Backup for AWS as described in section **Adding IAM Roles**. The list shows only IAM roles that belong to the production account — account where the file systems belong. Mind that, the specified IAM role must be included in one or more instance profiles. For more information on instance profiles, see **AWS Documentation**.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click **Check Permissions**. Veeam Backup for AWS will display the **Permission check** window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the **Missing Permissions** column. You can grant the missing permissions to the IAM role using the **AWS Management Console** or instruct Veeam Backup for AWS to do it.

   **TIP**

   To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click **Export Missing Permissions**.

   **IMPORTANT**

   If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see **AWS Documentation**.

To let Veeam Backup for AWS grant the missing permissions:

1. In the **Permission check** window, click **Grant**.

2. In the **Grant permissions** window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click **Apply**.

   The IAM user must have the following permissions:

   ```json
   "iam:CreatePolicy",
   "iam:GetRole",
   "iam:GetPolicy",
   "iam:AttachRolePolicy"
   ```
NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click **Recheck**.
Step 5. Configure Backup Target Settings

By default, backup policies create only backups of processed EFS file systems. At the **Targets** step of the wizard, you can specify backup vaults that will be used to store EFS backups and enable additional data protection scenarios:

- Specify backup vaults where Veeam Backup for AWS will store EFS file system backups.
- Instruct Veeam Backup for AWS to copy EFS file system backups to other AWS Regions.

Configuring Backup Settings

To specify backup vaults used to store backups of the selected EFS file systems, do the following:

1. In the **Backups** section of the **Targets** step of the wizard, click **Choose backup vaults**.
2. In the **Choose backup vaults** window, for each AWS Region included in the policy, specify a backup vault to save and organize file system backups. To do that:
   a. Select an AWS Region and click **Edit**.
   b. In the **Edit Backup Vault** window, from the **Backup vault** drop-down list, select the necessary backup vault.

      For a backup vault to be displayed in the **Backup vault** list, it must be created in the AWS Backup console as described in **AWS Documentation**. If you have not created a backup vault for the selected AWS Region, Veeam Backup for AWS will display only the default backup vault existing in this region.
   c. Click **Save**.
3. To save changes made to the backup policy settings, click **Apply**.

Enabling Additional Backup Copy

If you want to copy EFS file system backup to other AWS Regions, do the following:

1. In the **Backup copies** section of the **Targets** step of the wizard, set the **Create backup copies** toggle to **On**.
2. In the **Choose backup vaults** window, configure the following mapping settings for each AWS Region where original file systems reside:

   a. Select a source AWS Region in the list and click **Edit Region Mapping**.

   b. In the **Edit Region Mapping** window, specify the following settings:

      i. From the **Target region** drop-down list, select the target AWS Region to which Veeam Backup for AWS must copy created backups of the selected file systems.

      ii. From the **Backup vault** drop-down list, select a backup vault that will be used to store the copied backups.

         For a backup vault to be displayed in the **Backup vault** list, it must be created in the AWS Backup console as described in [AWS Documentation](#). If you have not created a backup vault for the selected AWS Region, Veeam Backup for AWS will display only the default backup vault existing in this region.

      iii. Click **Save**.

   To configure mapping for all source AWS Regions at once, click **Set Mapping for All Regions** and specify settings as described in **step 2.b**.

   c. To save changes made to the backup policy settings, click **Apply**.
Step 6. Specify Policy Scheduling Options

You can instruct Veeam Backup for AWS to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data stored in file systems added to the backup policy must be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for AWS allows you to create schedules of the following types:

- **Daily** — the backup policy will create restore points repeatedly throughout a day on specific days.
- **Weekly** — the backup policy will create restore points once a day on specific days.
- **Monthly** — the backup policy will create restore points once a month on a specific day.
- **Yearly** — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time. For more information, see Enabling Harmonized Scheduling.

**NOTE**

If you do not specify the backup schedule, after you configure the backup policy, you will need to start it manually to create EFS file system backups. For information on how to start backup policies, see Starting and Stopping Policies.

Specifying Daily Schedule

To create a daily schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Daily schedule** toggle to **On** and click **Edit Daily Settings**.

2. In the **Create daily schedule** window, select hours when the backup policy must create file system backups and backup copies.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on workdays (Monday through Friday) or on specific days.

4. In the **Daily retention** section, configure retention policy settings for the daily schedule. For backups and backup copies, specify the number of days (or months) for which you want to keep restore points in a backup chain.

**NOTE**

Veeam Backup for AWS does not create backup copies independently from file system backups. That is why when you select hours for backup copies, the same hours are automatically selected for backups. To learn how Veeam Backup for AWS performs backup, see EFS Backup.

5. If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see EFS Backup Retention.
5. To save changes made to the backup policy settings, click **Apply**.

### Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Weekly schedule** toggle to **On** and click **Edit Weekly Settings**.
2. In the **Create weekly schedule** window, select weekdays when the backup policy must create file system backups and backup copies.

**NOTE**

Veeam Backup for AWS does not create backup copies independently from file system backups. That is why when you select days to create backup copies, the same days are automatically selected for backups. To learn how Veeam Backup for AWS performs backup, see [EFS Backup](#).

3. Use the **Create restore point at** drop-down list to schedule a specific time for the backup policy to run.
4. In the **Weekly retention** section, configure retention policy settings for the weekly schedule. For backups and backup copies, specify the number of days (or months) for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see [EFS Backup Retention](#).
5. To save changes made to the backup policy settings, click Apply.

Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Monthly schedule toggle to On and click Edit Monthly Settings.
2. In the Create monthly schedule window, select months when the backup policy must create file system backups and backup copies.

NOTE

Veeam Backup for AWS does not create backup copies independently from EFS backups. That is why when you select hours for backup copies, the same hours are automatically selected for backups. To learn how Veeam Backup for AWS performs backup, see EFS Backup.

3. Use the Create restore point at and Run on drop-down lists to schedule a specific time and day for the backup policy to run.

NOTE

Consider the following:

- If you have selected a specific time for the backup policy to run at the Weekly schedule section of the Schedule step of the wizard, you will not be able to change the time for the monthly schedule unless you select the On Day option from the Run on drop-down list.
- If you select the On day option, harmonized scheduling cannot be guaranteed. Plus, to support the On day option, Veeam Backup for AWS will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed by the Backup Retention process from the AWS infrastructure during approximately 24 hours, to reduce unexpected infrastructure charges.
4. In the **Monthly retention** section, configure retention policy settings for the monthly schedule. For backups and backup copies, specify the number of days (or months) for which you want to keep restore points in a backup chain.

If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see [EFS Backup Retention](#).

5. To save changes made to the backup policy settings, click **Apply**.

---

**Specifying Yearly Schedule**

The yearly schedule is applied only to EFS file system backups, no backup copies are created according to this schedule.

To create a yearly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Yearly schedule** toggle to **On** and click **Edit Yearly Settings**.

2. In the **Create yearly schedule** window, specify a day, month and time when the backup policy must create file system backups.

   For example, if you select **First, Friday, January** and **06:00 PM**, the backup policy will run every first Friday of January at 06:00 PM.
NOTE

Consider the following:

- If you have selected a specific time for the backup policy to run at the Weekly schedule or Monthly schedule sections of the Schedule step of the wizard, you will not be able to change the time for the yearly schedule unless you select the On Day option from the Create restore point on drop-down list.
- If you select the On day option, harmonized scheduling cannot be guaranteed. Plus, to support the On day option, Veeam Backup for AWS will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed by the Backup Retention process from the AWS infrastructure during approximately 24 hours, to reduce unexpected infrastructure charges.

3. In the Keep backups for field, specify the number of years for which you want to keep restore points in a backup chain.
   
   If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore from the chain. For more information, see EFS Backup Retention.

4. To save changes made to the backup policy settings, click Apply.

Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for AWS applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of retaining restore points.

With harmonized scheduling, Veeam Backup for AWS can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time: EFS backups and backup copies can be kept for weeks, months and years.
For Veeam Backup for AWS to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of storing restore points. In terms of harmonized scheduling, Veeam Backup for AWS re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (D) flag is used to mark restore points created daily, (W) — weekly, (M) — monthly, and (Y) — yearly. Veeam Backup for AWS uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

Consider the following example. You want a backup policy to create backups of your file systems 1 time a day, to keep 3 daily backups in the backup chain, and also to keep one of the created backups for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

- In the daily scheduling settings, you select hours and days when backups must be created (for example, 7:00 AM, Working Days), and specify a number of days for which you want to keep daily restore points in a backup chain (for example, 3).

Veeam Backup for AWS will propagate these settings to the schedule of a less-frequent schedule (which is the weekly schedule in our example).
• In the weekly scheduling settings, you specify which one of the backups created by the daily schedule must be retained for a longer period, and choose for how long you want to keep the selected backup.

For example, if you want to keep the daily restore point created on Monday for 2 weeks, you select 7:00 AM, Monday and specify 14 days to keep in the weekly schedule settings.

According to the specified scheduling settings, Veeam Backup for AWS will create EFS backups in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) flag as it was created according to the daily schedule.

   Since 7:00 AM, Monday is specified in weekly schedule settings, Veeam Backup for AWS will assign the (W) flag to this restore point.

2. On the same week, after backup sessions run on Tuesday and Wednesday, the created restore points will be marked with the (D) flag.
3. On the fourth work day (Thursday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

By this moment, the earliest restore point in the backup chain will get older than the specified retention limit. However, Veeam Backup for AWS will not remove the earliest restore point (7:00 AM, Monday) with the (D) flag from the backup chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for AWS will unassign the (D) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

4. On the fifth working day (Friday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (D) flag.

By this moment, the restore point created on Tuesday with the (D) flag will get older than the specified retention limit. Veeam Backup for AWS will remove from the backup chain the restore point created at 7:00 AM on Tuesday as no flags of a less-frequent schedule are assigned to this restore point.

5. Veeam Backup for AWS will continue creating restore points for the next week in the same way as described in steps 1–4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the earliest weekly restore point in the backup chain will get older than the specified retention limit. Veeam Backup for AWS will unassign the (W) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for AWS will remove this restore point from the backup chain.
Step 7. Enable AWS Tags Assigning

At the Tags step of the wizard, choose whether you want to assign AWS tags to backups and backup copies.

- To assign already existing AWS tags from the processed EFS file systems, select the Copy tags from source file systems check box.

  If you choose to copy tags from source file systems, Veeam Backup for AWS will first create a backup or backup copy of the EFS file system and assign to the created backup AWS tags with Veeam metadata, then Veeam Backup for AWS will copy tags from the processed file system and, finally, assign the copied AWS tags to the backup.

- To assign your own custom AWS tags, set the Add custom tags to created backups toggle to On and specify the AWS tags explicitly. To do that, use the Key and Value fields to specify a key and a value for the new custom AWS tag, and then click Add. Note that you cannot add more than 5 custom AWS tags.

  If you choose to add custom tags to created snapshots, Veeam Backup for AWS will assign the specified tags right after it creates a backup or backup copy.
Step 8. Specify Retry and Email Notification Settings

At the **General Settings** step of the wizard, you can enable automatic retries and specify notification settings for the backup policy.

### Automatic Retry Settings

To instruct Veeam Backup for AWS to run the backup policy again if it fails on the first try, do the following:

1. In the **Schedule** section of the step, select the **Automatically retry failed policy** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 60 seconds.

When retrying backup policies, Veeam Backup for AWS processes only those file systems that failed to be backed up during the previous attempt.

### Email Notification Settings

**NOTE**

To be able to specify email notification settings for the EFS Backup policy, you must configure the SMTP server settings first. For more information on how to configure the SMTP server settings, see [Configuring Global Email Notification Settings](#).

To instruct Veeam Backup for AWS to send email notifications for the backup policy, do the following:

1. In the **Notifications** section of the step, set the **Enabled** toggle to **On**.
   
   If you set the toggle to **Off**, Veeam Backup for AWS will send notifications according to the configured global notification settings.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.

3. Use the **Notify on** list to choose whether you want Veeam Backup for AWS to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

4. Select the **Suppress notifications until the last retry** check box to receive a notification about the final backup policy result.
   
   If you do not select the check box, Veeam Backup for AWS send a notification for every backup policy retry.
NOTE

If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for AWS will override the configured global notification settings and will send each notification to this recipient only once to avoid notification duplicates.
Step 9. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the Schedule step of the wizard]

At the Cost Estimation step of the wizard, review the estimated monthly cost of AWS services and resources that will be consumed to protect the instances added to the backup policy. The total estimated cost includes the following:

- The cost of creating backups of the EFS file systems.
  For each file system included in the backup policy, Veeam Backup for AWS takes into account the number of restore points to be kept in the backup chain and the configured scheduling settings.

- The cost of creating backup copies and maintaining them in the target AWS Region.
  For each file system included in the backup policy, Veeam Backup for AWS takes into account the number of restore points to be kept in the backup chain and the configured scheduling settings.

- The cost of sending API requests to Veeam Backup for AWS during data protection operations.

To calculate the estimated cost, Veeam Backup for AWS uses capabilities of the Amazon Web Services Simple Monthly Calculator.

The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and AWS backup charges. To reduce the cost, you can try the following workarounds:

- To reduce high AWS backup charges, adjust the backup retention settings to keep less restore points in the snapshot chain.

- To optimize the cost of storing backups, configure the scheduling settings to run the backup policy less frequently.
TIP
You can save the cost estimation as a .CSV or .XML file. To do that, click Export to and select the necessary format.

Related Resources
How AWS Pricing Works
Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, it is recommended that you run the backup policy configuration check before you click **Finish**.

The configuration check will verify whether specified IAM roles have all the required permissions, and networks settings are configured properly to launch worker instances. To run the check, click **Test Configuration**. Veeam Backup for AWS will display the **Test policy configuration** window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient or policy settings are not configured properly, the check will complete with errors, and the list of permissions that must be granted to the IAM role and policy configuration issues will be displayed in the **Test policy configuration** window.

You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

To let Veeam Backup for AWS grant the missing permissions:

1. In the **Test policy configuration** window, click the **Grant** link.
2. In the **Grant Permissions** window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click **Apply**.

   The IAM user must have the following permissions:

   ```
   "iam:CreatePolicy",
   "iam:GetRole",
   "iam:GetPolicy",
   "iam:AttachRolePolicy"
   ```

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. After the required permissions are granted, close the Test policy configuration window, and then click Finish to close the Add Policy wizard.

Veeam Backup for AWS will save the configured backup policy.
Creating EFS Backups Manually

Veeam Backup for AWS allows you to manually create backups of Amazon EFS file systems. You can instruct Veeam Backup for AWS to store the created backups in the same AWS Regions where the processed file systems reside, or in a different AWS Region.

**NOTE**

Veeam Backup for AWS does not include EFS backups created manually in the EFS backup chain and does not apply the configured retention policy settings to these backups. This means that the backups are kept in your AWS environment unless you remove them manually, as described in section Managing Backed-Up EFS Data.

To manually create a backup of an EFS file system, do the following:

1. Navigate to Resources > EFS.

   **NOTE**

   By default, Veeam Backup for AWS uses an AWS CloudTrail trail to track changes in your EFS resources. If no trails are configured in the source AWS account, Veeam Backup for AWS will access AWS resources and populate the list of available file systems or AWS tags only once in 24 hours. To force the data collection process manually, click Rescan.

2. Select the necessary file system and click Take Backup Now.

   For an EFS file system to be displayed in the list of available file systems, an AWS Region where the file system resides must be added to any of configured EFS backup policies, and the IAM role specified in the backup policy settings must have permissions to access the file system. For more information on required permissions, see EFS Backup IAM Role Permissions.

3. Complete the Take Manual Backup wizard:

   a. At the Account step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to create the backup.

      For an IAM role to be displayed in the list, it must be added to Veeam Backup for AWS as described in section Adding IAM Roles.

   b. In the Backup vault section of the Settings step of the wizard, click Edit Location Settings.

      In the Choose region and backup vault window, specify the following settings:

      i. From the Target region drop-down list, select an AWS Region where manual backups will be stored.

      ii. In the Backup vault section, select a backup vault that will be used to store file system backups.

      iii. To save changes made to the location settings, click Apply.

   c. At the Tags section of the Settings step of the wizard, if you want to assign tags to the created backup, click Edit Tag Settings.

      In the Tag configuration window, specify tag settings:
i. To assign already existing AWS tags from the processed file system, select the **Copy tags from source file system** check box.

If you choose to copy tags from source file system, Veeam Backup for AWS will first create a backup of the EFS file system and assign to the created backup AWS tags with Veeam metadata, then Veeam Backup for AWS will copy tags from the processed file system and, finally, assign the copied AWS tags to the backup.

ii. To assign your own custom AWS tags, set the **Add custom tags to created backup** toggle to **On** and specify the tags explicitly. To do that, use the **Key** and **Value** fields to specify a key and a value for the new custom AWS tag, and then click **Add**. Note that you cannot add more than 5 custom AWS tags.

If you choose to add custom tags to created backups, Veeam Backup for AWS will assign the specified tags right after it creates a backup.

iii. To save changes made to the tag settings, click **Apply**.

iv. At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing VPC Configuration Backup

To protect the Amazon VPC configuration and settings, Veeam Backup for AWS comes with a preconfigured VPC Configuration Backup policy. With this policy, you can protect VPC configurations of AWS Regions in your AWS accounts.

The VPC Configuration Backup policy is disabled by default. To start protecting your Amazon VPC configuration, edit backup policy settings and enable the policy.

IMPORTANT

Veeam Backup for AWS does not support backup of the following VPC configuration components: VPC Traffic Mirroring, AWS Network Firewall, VPC Flow Logs, carrier gateways, customer IP pools, and core networks in route tables.
Editing VPC Configuration Backup Policy

To configure the VPC Configuration Backup policy settings, complete the following steps:

1. Launch the VPC Configuration Backup wizard.
2. Select AWS Regions to protect.
3. Specify a backup repository to store an additional backup copy.
5. Specify automatic retry settings and notification settings.
6. Finish working with the wizard.
Step 1. Launch VPC Configuration Backup Wizard

To launch the VPC Configuration Backup wizard, complete the following steps.

1. Navigate to Policies > VPC.
2. Click Edit.
Step 2. Select AWS Regions

At the **Regions** step of the wizard, select AWS Regions whose VPC configuration you want to back up.

Veeam Backup for AWS allows you to automatically collect and back up VPC configuration data for all AWS Regions selected for EC2 and RDS backup policies. To do that, enable **automatic protection** for AWS Regions. To retrieve VPC configurations of all automatically protected AWS Regions, Veeam Backup for AWS will use permissions of IAM roles specified in the settings of backup policies that protect instances residing in these AWS Regions.

You can also configure the VPC Configuration Backup policy to protect configuration data for AWS Regions that are not specified in the settings of any backup policy, or choose another IAM role whose permissions Veeam Backup for AWS will use to collect the VPC configuration data of the automatically protected AWS Regions. To do that, manually add AWS Regions to the VPC Backup policy and configure backup settings for them.

### Enabling Automatic Protection

To instruct Veeam Backup for AWS to protect VPC configuration of all AWS Regions specified in EC2 and RDS backup policy settings, in the **Automatically protected regions** section, set the **Automatically collect VPC settings** toggle to **On**.

To retrieve VPC configurations of all automatically protected AWS Regions, Veeam Backup for AWS will use permissions of IAM roles specified in the settings of backup policies that protect instances residing in these AWS Regions. It is recommended that you check whether IAM roles whose permissions EC2 and RDS backup policies use to perform data protection operations have all the required permissions to perform Amazon VPC configuration backup. If the IAM role permissions are insufficient, the backup policy will fail.

To run the IAM role permission check:

1. In the **Automatically Protected Regions** section, click the **Discovered regions** link.
2. In the **Discovered regions** window, select the IAM role whose permissions you want to check.
3. Click **Check Permissions**.

Veeam Backup for AWS will display the **AWS Permission Check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column. For more information on required permissions, see **VPC Configuration Backup IAM Role Permissions**.

You can grant the missing permissions to the IAM role in the AWS Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to IAM roles using the AWS Management Console, see **AWS Documentation**. To let Veeam Backup for AWS grant the missing permissions:

a. In the **AWS Permission Check** window, click **Grant**.

b. In the **Grant Permissions Window**, provide one-time access keys of an IAM user that is authorized to update permissions of the IAM role, and then click **Apply**.

The IAM user whose access keys are used to update the IAM role must have the following permissions:

```
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"
```
NOTE
Veeam Backup for AWS does not store one-time access keys in the configuration database.

c. To make sure that the missing permissions were successfully granted, click Recheck.

Adding AWS Regions Manually

To add an AWS Region to the VPC Backup policy, or to choose another IAM role for collecting VPC configuration data, do the following:

1. In the Additional regions section, click Add.
2. In the Configure account settings window, from the IAM role drop-down list, select an IAM role whose permissions Veeam Backup for AWS must use to perform Amazon VPC configuration backup. In the Account field, the ID of the AWS account in which the IAM role was created will be displayed.
3. In the Regions section, select the necessary AWS Regions from the Available Regions list on the left, and then click Add.
4. To save changes made to the backup policy settings, click Apply.
5. To check whether IAM role specified for the selected AWS Regions has all the required permissions to perform Amazon VPC configuration backup, in the Additional regions section, click Check Permissions.
You can add, edit or remove additional AWS Regions from the VPC Backup policy.
Step 3. Enable Additional Backup Copy

By default, Veeam Backup for AWS store VPC configuration backups in the Veeam Backup for AWS database. You can instruct Veeam Backup for AWS to save additional VPC configuration backup copies to a backup repository. To do that:

1. At the **Target** step of the wizard, set the **Enable additional copy** toggle to **On**.

2. In the **Repository** window, specify a backup repository that will be used to store the additional configuration backup copies.

3. To save changes made to the backup policy settings, click **Apply**.

If you want to encrypt the VPC configuration data stored in a backup repository, enable encryption on the repository level. For more information, see Adding Backup Repositories.
Step 4. Configure Retention Settings

At the **Retention** step of the wizard, specify retention settings for VPC configuration backups.

1. Click the **Collect data** link.

2. In the **Daily retention** window, specify how often the data must be backed up and for how long the backups must be stored.

   If a restore point is older than the specified time limit, Veeam Backup for AWS removes the restore point from the chain. For more information, see [VPC Configuration Backup Retention](#).

**NOTE**

Veeam Backup for AWS applies the retention settings configured for the VPC Configuration Backup policy both to VPC configuration backups stored in the Veeam Backup for AWS database and to VPC configuration backups stored in the backup repository selected for the policy. For VPC configuration backups stored in backup repositories that are not specified in the VPC Configuration Backup policy settings, Veeam Backup for AWS applies retention settings saved in the backup metadata.
Step 5. Specify Email Notification Settings

At the **Settings** step of the wizard, you can specify email notification settings for the VPC Backup policy.

**NOTE**

To be able to specify email notification settings for the VPC Configuration Backup policy, you must configure the SMTP server settings first. For more information on how to configure the SMTP server settings, see Configuring Global Email Notification Settings.

To instruct Veeam Backup for AWS to send email notifications for the backup policy, do the following:

1. In the **Notifications** section, set the **Receive daily report** toggle to **On**.
   
   If you set the toggle to **Off**, Veeam Backup for AWS will send notifications according to the configured **global notification settings**.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.

3. Use the **Notify on** list to choose whether you want Veeam Backup for AWS to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

**NOTE**

If you specify the same email recipient in both backup policy notification and **global notification settings**, Veeam Backup for AWS will override the configured **global notification settings** and will send each notification to this recipient only once to avoid notification duplicates.
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.
Enabling and Disabling VPC Configuration Backup Policy

By default, Veeam Backup for AWS comes with the disabled VPC Configuration Backup Policy. You can manually start or enable the disabled backup policy at any time you need.

To enable or disable the VPC Configuration Backup policy, do the following:

1. Navigate to Policies > VPC.

2. Click Enable or Disable.
Starting and Stopping VPC Configuration Backup Policy

You can start the VPC Configuration Backup policy manually, for example, if you want to create an additional restore point in the backup chain and do not want to modify the configured backup policy schedule. You can also stop a backup policy if the backup process is about to take long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop a backup policy, do the following:

1. Navigate to Policies > VPC.
2. Click **Start** or **Stop**.
Managing EC2, RDS and EFS Backup Policies

You can manage and edit created EC2, RDS and EFS backup policies, and view each backup policy details in Veeam Backup for AWS. You can also remove backup policies that you do not use anymore, export existing or import new backup policies.
Starting and Stopping Policies

You can start a backup policy manually, for example, if you want to create an additional restore point in the snapshot or backup chain and do not want to modify the configured backup policy schedule. You can also stop a backup policy if processing of an instance is about to take too long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop a backup policy, do the following:

1. Navigate to Policies.
2. Switch to the necessary tab and select the backup policy.
3. Click Start or Stop.
Disabling and Enabling Policies

By default, Veeam Backup for AWS runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for AWS does not run the backup policy automatically. You will still be able to manually start or enable the disabled backup policy at any time you need.

To enable or disable a backup policy, do the following:

1. Navigate to **Policies**.
2. Switch to the necessary tab and select the backup policy.
3. Click **Disable** or **Enable**.
Setting Policy Priority

You can set priority for backup policies created in Veeam Backup for AWS. If an instance or a file system is included into several backup policies, it will be processed only by one backup policy that has the highest priority.

To set priority for backup policies:

1. Navigate to Policies.
2. Switch to the necessary tab and click Policy Priority.
3. In the Priority Order window, use the Up and Down arrows to set priority for backup policies, and click Apply to save the settings.

The first backup policy in the list will have the highest priority.
Editing Policy Settings

You can edit backup policies created in Veeam Backup for AWS. For example, you may want to add some resources to a backup policy, change a backup policy description and so on.

**TIP**

To protect additional resources by a configured backup policy, you can either edit the resource list in the backup policy settings, or add resources to the backup policy on the Resources tab. To learn how to add resources on the Resources tab, see Adding Resources to Policy.

To edit backup policy settings:

1. Navigate to Policies.
2. Switch to the necessary tab and select the backup policy whose settings you want to edit.
3. Click Edit. The Edit Policy wizard will open.
Exporting and Importing Policies

Veeam Backup for AWS allows you to use settings of an existing backup policy as a template for creating other backup policies. You can export a backup policy to a .JSON file, modify the necessary settings in the file, and then import the policy to the same or a different backup appliance.

Exporting Backup Policies

To export a backup policy to a .JSON file:

1. Navigate to Policies.
2. Switch to the necessary tab and select the backup policy whose settings you want to export.
3. Click Advanced > Export Policy.

Veeam Backup for AWS will save the backup policy settings as a single .JSON file to the default download directory on the local machine.

Importing Backup Policies

To import a backup policy from a .JSON file:

1. Navigate to Policies.
2. Switch to the necessary tab and click Advanced > Import Policy.
3. In the **Import Policy** window, specify a name for the imported backup policy, paste the content of the necessary .JSON file, and click **Apply**.
Managing Backed-Up Data

Veeam Backup for AWS stores information on all protected AWS resources in the configuration database. Even if a resource is no longer protected by any configured backup policy and even if the resource no longer exists in the AWS infrastructure, information on the backed-up data will not be deleted from the database until Veeam Backup for AWS automatically removes all restore points associated with this resource according to the retention settings saved in the backup metadata. You can also remove the restore points manually on the Protected Data page.

NOTE

Veeam Backup for AWS does not include restore points created manually in backup and snapshot chains, and does not apply the configured retention policy settings to these restore points. This means that the restore points are kept in your AWS environment unless you remove them manually, as described in sections Removing EC2 Snapshots Created Manually, Removing RDS Snapshots Created Manually and Removing EFS Backups Created Manually.
Managing Backed-Up EC2 Data

To view and manage backed-up EC2 instance data, navigate to Protected Data > EC2. The EC2 tab displays information on all protected EC2 instances and allows you to remove restore points of the instances if you no longer need them.

For each backed-up EC2 instance, Veeam Backup for AWS creates a record in the configuration database with the following set of properties:

- **Instance** — a name of an EC2 instance.
- **Policy** — a name of the backup policy that processed the EC2 instance.
- **Restore Points** — a number of restore points created for the EC2 instance.
- **Latest Restore Point** — the date and time of the latest restore point that was created for the EC2 instance.
- **Instance Size** — a size of all EBS volumes attached to the EC2 instance.
- **Region** — an AWS Region in which the EC2 instance resides.
- **Data Retrieval** — shows whether any of the archived restore points of the EC2 instance is retrieved.
- **File-level Recovery URL** — a link to the file-level recovery browser.
  
  The link appears when the restore session is started for the file-level restore process. The link contains a public DNS name of the worker instance hosting the file-level recovery browser and authentication information used to access this worker instance.
- **Operating System** — an operating system running on the EC2 instance.
- **IAM Role** — an IAM Role used to back up the EC2 instance.
- **AWS Account** — an AWS account where the EC2 instance belong.
- **Instance ID** — an AWS ID of the EC2 instance.
Removing EC2 Backups and Snapshots

Veeam Backup for AWS applies the configured retention policy settings to automatically remove cloud-native snapshots, snapshot replicas and image-level backups created by backup policies. If necessary, you can also remove the backed-up data manually.

**IMPORTANT**
Do not delete backup files from Amazon S3 buckets in the AWS Management Console. If some file in a backup chain is missing, you will not be able to roll back EC2 instance data to the necessary state.

To remove backed-up data manually, do the following:

1. Navigate to Protected Data > EC2.
2. Select EC2 instances whose data you want to remove.
3. Click Remove and select either of the following options:
   - **Snapshots > All** — to remove all cloud-native snapshots and snapshot replicas created for the selected EC2 instances both by backup policies and manually.
   - **Snapshots > Manual** — to remove cloud-native snapshots created for the selected EC2 instances manually.
     If you want to remove only specific cloud-native snapshots, follow the instructions provided in section Removing Snapshots Created Manually.
   - **Snapshots > Local** — to remove cloud-native snapshots created for the selected EC2 instances by backup policies.
   - **Snapshots > Replica** — to remove snapshot replicas created for the selected EC2 instances by backup policies.
   - **Backups > All** — to remove all backups created for the selected EC2 instances.
   - **Backups > Standard** — to remove all standard backups created for the selected EC2 instances.
   - **Backups > Archived** — to remove all archived backups created for the selected EC2 instances.
   - **Snapshots and Backups** — to remove cloud-native snapshots, snapshot replicas, and image-level backups created for the selected EC2 instances.
Removing EC2 Snapshots Created Manually

To remove all cloud-native snapshots created for an EC2 instance manually, follow the instructions provided in the Removing EC2 Backups and Snapshots section. If you want to remove a specific snapshot created manually, do the following:

1. Navigate to Protected Data > EC2.
2. Select the necessary instance, and click the link in the Restore Points column.
3. In the Available Restore Points window, select a snapshot that you want to remove, and click Remove Manual Snapshot.
Retrieving Data From Archive

Backups stored in archive repositories are not immediately accessible. If you want to restore an EC2 instance from a backup that is stored in a repository with the S3 Glacier or S3 Glacier Deep Archive storage class, you must first retrieve the archived data. During the data retrieval process, a temporary copy of the archived data is created in an Amazon S3 bucket where the repository located. This copy is stored in the S3 standard storage class for a period of time that you specify when launching the data retrieval process. If the time period expires while a restore operation is still running, Veeam Backup for AWS automatically extends the period to keep the retrieved data available for 1 more day. You can also extend the availability period manually.

To retrieve archived data, you can launch the data retrieval process either from the Data Retrieval wizard before you begin a restore operation, or directly from the Restore wizard. When you retrieve archived data, you can choose one of the following options:

- **Expedited** – the most expensive option. The retrieved data is available within 1–5 minutes. Amazon does not support this option for data stored in the S3 Glacier Deep Archive storage class. For details, see AWS Documentation.

- **Standard** – the recommended option. The retrieved data is available within 3–5 hours for data stored in the Amazon S3 Glacier storage class and within 12 hours for data stored in the Amazon S3 Glacier Deep Archive storage class.

- **Bulk** – the least expensive option. The retrieved data is available within 5–12 hours for data stored in the Amazon S3 Glacier storage class and within 48 hours for data stored in the Amazon S3 Glacier Deep Archive storage class.

For more information on archive retrieval options, see AWS Documentation.

Retrieving Data Manually

To retrieve archived data of an EC2 instance, do the following:

1. Navigate to Protected Data > EC2.
2. Select the necessary instance, and click the link in the Restore Points column.
3. In the Available Restore Points window, select a restore point that contains archived data you want to retrieve, and click Retrieve Backup. The Data Retrieval wizard will open.
4. At the **Settings** step of the wizard, specify the following settings:

   a. In the **Retrieval mode** section, select the **retrieval option** that Veeam Backup for AWS will use to retrieve the data.

   b. In the **Availability period** section, specify the number of days for which you want to keep the data available for restore operations.

   You will be able to **manually extend data availability** later if required.

   **TIP**

   If you want to receive an email notification when data availability period is about to expire, select the **Send notification email** check box, and specify the number of hours before the expiration time when the notification must be sent.

5. At the **Summary** step of the wizard, review configuration information and click **Finish**.
IMPORTANT

If you cancel the Data Retrieval session, or the Veeam Backup for AWS service is restarted while the Data Retrieval session is still running, AWS will retrieve data anyway and keep it for the specified availability period. However, Veeam Backup for AWS will not be able to access the retrieved data.

Extending Data Availability

To extend time for which you want to keep retrieved data available for restore operations:

1. Navigate to Protected Data > EC2.
2. Select the EC2 instance for which you want to extend availability of the retrieved data.
3. Click Extend Availability.
   Alternatively, click the link in the Restore Points column. In the Data Retrieval window, select the restore point that contains the retrieved data, and click Extend Availability.
4. In the Extend Data Availability Period window, specify the number of days for which you want to keep the data available for restore operations, and click Extend.
Managing Backed-Up RDS Data

To view and manage backed-up RDS data, navigate to Protected Data > RDS. The RDS tab displays information on all protected DB instances and Aurora DB clusters and allows you to remove restore points of the instances if you no longer need them.

For each backed-up RDS resource, Veeam Backup for AWS creates a record in the configuration database with the following set of properties:

- **Instance** — a name of a DB instance or an Aurora DB cluster.
- **Policy** — a name of the backup policy that processed the DB instance or Aurora DB cluster.
- **Snapshots** — a number of snapshots created for the DB instance or Aurora DB cluster.

**NOTE**

Veeam Backup for AWS displays all existing snapshots of RDS resources, not only snapshots created by the Veeam backup service. Amazon DB snapshots created for DB instances or Aurora DB clusters in AWS have the AWS Snapshot type and cannot be deleted from the Veeam Backup for AWS Web UI.

- **Latest Snapshot** — the date and time of the latest snapshot that was created for the DB instance or Aurora DB cluster.
- **Engine** — a database engine of the DB instance or Aurora DB cluster.
- **Instance Size** — a size of the DB instance storage.
- **Region** — an AWS Region in which the DB instance or Aurora DB cluster resides.
- **AWS Account** — an AWS account where the DB instance or Aurora DB cluster belong.
- **Instance ID** — an AWS ID of the DB instance or Aurora DB cluster.
Removing RDS Snapshots

Veeam Backup for AWS applies the configured retention policy settings to automatically remove cloud-native snapshots and snapshot replicas created by backup policies. If necessary, you can also remove the backed-up data manually.

**NOTE**

In Veeam Backup for AWS, you can remove only snapshots created by the Veeam backup service. To delete AWS Snapshots (DB instance snapshots created in AWS), use Amazon Management Console.

To remove backed-up data manually, do the following:

1. Navigate to Protected Data > RDS.
2. Select RDS resources whose data you want to remove.
3. Click Remove and select either of the following options:
   - **All** — to remove all cloud-native snapshots and snapshot replicas created for the selected RDS resources both by backup policies and manually.
   - **Manual Snapshots** — to remove cloud-native snapshots created for the selected RDS resources manually.
   - **Local Snapshots** — to remove cloud-native snapshots created for the selected RDS resources by backup policies.
     
     If you want to remove only specific cloud-native snapshots, follow the instructions provided in section Removing RDS Snapshots Created Manually.
   - **Replicas** — to remove snapshot replicas created for the selected RDS resources by backup policies.
Removing RDS Snapshots Created Manually

To remove all cloud-native snapshots created for a DB instance or an Aurora DB cluster manually, follow the instructions provided in the Removing RDS Snapshots section. If you want to remove a specific snapshot created manually, do the following:

1. Navigate to Protected Data > RDS.
2. Select the necessary resource, and click the link in the Snapshots column.
3. In the Available Restore Points window, select a snapshot that you want to remove, and click Remove Manual Snapshot.
Managing Backed-Up EFS Data

To view and manage backed-up EFS file system data, navigate to Protected Data > EFS. The EFS tab displays information on all protected EFS file systems and allows you to remove restore points of the file systems if you no longer need them.

For each backed-up Amazon EFS file system, Veeam Backup for AWS creates a record in the configuration database with the following set of properties:

- **Name** — a name of an EFS file system.
- **Policy** — a name of the backup policy that processed the EFS file system.
- **Restore Points** — a number of restore points created for the EFS file system.
- **Latest Restore Point** — the date and time of the latest restore point that was created for the EFS file system.
- **Total Size** — a size of the EFS file system storage.
- **Region** — an AWS Region in which the EFS file system resides.
- **AWS Account** — an AWS account where the EFS file system belong.
- **File System ID** — an AWS ID of the EFS file system.
- **File-level Recovery URL** — a link to the file-level recovery browser.

The link appears when the restore session is started for the file-level restore process. The link contains a public DNS name or an IP address of the backup appliance hosting the file-level recovery browser and authentication information used to access the appliance.
Removing EFS Backups

Veeam Backup for AWS applies the configured retention policy settings to automatically remove EFS file system backups and backup copies created by backup policies. If necessary, you can also remove the backed-up data manually.

To remove backed-up data manually, do the following:

1. Navigate to Protected Data > EFS.
2. Select EFS file systems whose data you want to remove.
3. Click Remove and select either of the following options:
   - **Backups** — to remove EFS backups created for the selected file systems by backup policies.
   - **Backup Copies** — to remove backup copies created for the selected file systems by backup policies.
   - **Manual Backups** — to remove EFS backups created for the selected file systems manually.

   If you want to remove only specific manual backup, follow the instructions provided in section Removing EFS Backups Created Manually.

   - **All** — to remove all backups and backup copies created for the selected file systems both by backup policies and manually.
Removing EFS Backups Created Manually

To remove all backups created for an EFS file system manually, follow the instructions provided in the Removing EFS Backups section. If you want to remove a specific EFS backup created manually, do the following:

1. Navigate to Protected Data > EFS.
2. Select the necessary file system, and click the link in the Restore Points column.
3. In the Available Restore Points window, select a backup that you want to remove, and click Remove Manual Backups.
Managing Backed-Up VPC Configuration Data

To view and manage backed-up VPC configuration data, navigate to Protected Data > VPC. The VPC tab displays information on all saved VPC configurations, and allows you to export the configurations and to remove configuration restore points if you no longer need them.

For each protected AWS Region within the AWS account, Veeam Backup for AWS creates a configuration record in the database. To view all existing configuration records, navigate to Protected Data > VPC.

Each configuration record is described with a set of properties:

- **AWS Account** – a name of an AWS account whose IAM role was used to collect VPC configuration data.
- **Region** – an AWS Region whose VPC configuration data is backed up.
- **Latest Backup** – the date and time of the latest created restore point.
- **Latest Changes** – the summary of changes in the VPC configuration in comparison with the previous restore point.
- **Restore Points** – a number of restore points created for the VPC configuration.

In the Configuration details section, Veeam Backup for AWS displays the backed-up VPC configuration details for the selected configuration record.

You can export, compare and remove backed-up Amazon VPC configuration data.
Removing VPC Configuration Backups

Veeam Backup for AWS applies the configured retention policy settings to automatically remove VPC configuration backups created by the VPC Configuration Backup policy. If necessary, you can also remove the backed-up data manually.

**IMPORTANT**

If you remove a configuration record for an AWS Region, all VPC configuration backups for the selected AWS Region will be removed.

To remove backed-up data manually, do the following:

1. Navigate to Protected Data > VPC.
2. Select the configuration record for which you want to remove the backed-up data.
3. Click Remove and select either of the following options:
   - **Backups** — to remove all VPC configuration backups for the selected configuration record from the Veeam Backup for AWS database.
   - **Backup Copies** — to remove all VPC configuration backups for the selected configuration record from the backup repository, specified in the target settings of the VPC Configuration Backup policy.

**NOTE**

If you remove Amazon VPC configuration backups from the Veeam Backup for AWS database but leave their additional copies in any backup repository, these backups will be added back to the Veeam Backup for AWS database when the Veeam backup service restarts or Veeam Backup for AWS rescans the repository.

![Configuration Details](image-url)
Comparing VPC Configuration Backups

You can compare the current Amazon VPC configuration of an AWS Region to the backed-up Amazon VPC configuration.

1. Navigate to Protected Data > VPC.
2. Select the configuration record for an AWS Region whose VPC configuration you want to compare.
3. Click Compare.

By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can compare the VPC configuration data to an earlier state. In the Compare Attributes window, click the link to the right of Restore point to select the necessary restore point.

If you want Veeam Backup for AWS to display only backed-up VPC configuration items that differ from the current VPC configuration items, set the Show only changed attributes toggle to On.

You can export or restore the VPC configuration using the selected restore point:

- To export the entire VPC configuration, click Export and follow the instructions provided in Performing Entire Configuration Export.
- To restore the entire VPC configuration, click Restore and follow the instructions provided in Performing Entire Configuration Restore.
Exporting VPC Configuration

You can export backed-up VPC configuration data to an AWS CloudFormation template in the JSON format using one of the following options:

- Perform the entire VPC configuration export.
- Perform the selected VPC configuration items export.

Performing Entire Configuration Export

You can export the entire VPC configuration and restore it from the CloudFormation template to the original location or to a new location.

**IMPORTANT**

If you plan to restore the exported VPC configuration, consider that restore to a new location is not supported for the following VPC configuration items:

- Client VPN endpoints.
- Customer gateways and load balancer listeners that use authentication certificates.
- In route tables, for core networks and routes to AWS Outpost local gateways, network interfaces, instances and carrier gateways.

To export the entire VPC configuration to a CloudFormation template, complete the following steps:

1. Launch the VPC Export wizard.
2. Select a restore point and VPCs to export.
3. Specify an IAM identity for export.
4. Choose an export mode.
5. Configure mapping for Availability Zones.
6. Configure settings for VPC peering connections.
7. Specify an Amazon S3 bucket where the CloudFormation template must be placed.
8. Specify a reason for export.
Step 1. Launch VPC Export Wizard

To launch the **VPC Export** wizard, complete the following steps.

1. Navigate to **Protected Data** > **VPC**.
2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.
3. Click **Export** > **Entire VPC**.

![VPC Export Wizard Image]
Step 2. Select Restore Point

At the **Export List** step of the wizard, select the VPC whose configuration you want to export and a restore point that will be used to export the selected VPC configuration. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can export the VPC configuration data to an earlier state.

To select a restore point, do the following:

1. In the **Choose restore point** section, click the link to the right of **Restore point**.
2. In the **Available restore points** window, select the necessary restore point and click **Apply**.
3. In the **Choose VPCs to export** section, select VPCs whose configuration you want to export.
Step 3. Specify IAM Identity

At the **Account** step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to perform the export operation.

**IMPORTANT**

Make sure, that the specified IAM role belongs to an AWS account in which you plan to restore the VPC configuration.

To specify an IAM role for export, select the necessary IAM role from the list. For an IAM role to be displayed in the list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **VPC Export** wizard. To add an IAM role, click **Add** and complete the **Add IAM Role** wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform export. To run the IAM role permission check, click **Check Permissions**. Veeam Backup for AWS will display the **Permission check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column.

You can grant the missing permissions to the IAM role in the AWS Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to IAM roles using the AWS Management Console, see **AWS Documentation**.
Step 4. Choose Export Mode

At the **Export Mode** step of the wizard, choose whether you plan to restore the exported VPC configuration to the original or to a custom location. If you select the **Export to a new location** option, specify the target AWS Region where the VPC configuration will be restored.

**IMPORTANT**

Before you choose the export mode, consider the following:

- If you plan to restore the exported VPC configuration to the original location — when you restore the VPC configuration from the CloudFormation template, all exported VPC configuration items will be newly created in the source AWS Region. If there are any already existing items with the same names in the current VPC configuration, the restored items will be created with new IDs, but with the same names.

- If you plan to restore the exported VPC configuration to a custom location — the source and target AWS Regions may have different lists of the supported AWS services. In this case, when you restore the VPC configuration from the CloudFormation template, VPC endpoints created using an AWS service that is not available in the target AWS Region will not be restored.
Step 5. Configure Availability Zone Mapping

[This step applies only if you have selected the Export to a new location option at the Export Mode step of the wizard]

At the Availability Zones step of the wizard, for each source Availability Zone, choose an Availability Zone in the target AWS Region where VPC configuration items of the source Availability Zone will be restored:

1. Choose an Availability Zone from the list and click Edit Mapping.
2. In the Map availability zone window, select the target Availability Zone from the Target region drop-down list.
3. Click Apply.

**IMPORTANT**

The source and target AWS Regions may have different number of Availability Zones. In this case, Veeam Backup for AWS will automatically change subnet configuration for transit gateway VPC attachments, VPC endpoints and load balancers. After restoring, you can modify the subnet configuration manually in the AWS Management Console. To learn how to modify subnet configuration for VPC networking components, see AWS Documentation.
Step 6. Configure Peering Connection Settings

[This step applies only if you have selected the Export to a new location option at the Export Mode step of the wizard]

At the Peering Connection step of the wizard, review VPC peering connection settings. You cannot modify the VPC peering connection settings for the exported VPC. By default, Veeam Backup for AWS will export VPC peering connections as follows:

- If you export both VPCs between which you have created a peering connection, Veeam Backup for AWS will create a peering connection between the exported VPCs in the target AWS Region.

- If you export a VPC that has a peering connection to a VPC in the same AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the exported VPC in the target AWS Region and the VPC with which the source VPC is peered in the source AWS Region.

- If you export a VPC that has a peering connection to a VPC in another AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the exported VPC in the target AWS Region and the VPC with which the source VPC is peered in the other AWS Region.

NOTE

VPC peering connections will have the Pending Acceptance status after restoring from the exported CloudFormation template. To accept the restored VPC peering connections, use the AWS Management Console. For more information, see AWS Documentation.
Step 7. Specify Amazon S3 Bucket

At the Target step of the wizard, specify an Amazon S3 bucket where Veeam Backup for AWS will save the CloudFormation template with the exported VPC configuration data.

Choose whether you want to save the template in the root folder of the selected Amazon S3 bucket or to create a new folder for the template.
Step 8. Specify Export Reason

At the **Reason** step of the wizard, specify a reason for the export of the VPC configuration. The information you provide will be saved in the session history and you can reference it later.

Export reason

Specify a reason for performing the export operation.

Export reason:

Export of VPC configuration: vpc-0d8b332140042512
Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

**Performing Selected Items Export**

**NOTE**

If you export only specific VPC configuration items, you will not be able to choose a location. By default, Veeam Backup for AWS will create a CloudFormation template to restore to the original location.

When you restore the exported items from the CloudFormation template, all exported VPC configuration items will be newly created in the source AWS Region. If there are any already existing items with the same names in the current VPC configuration, the restored items will be created with new IDs, but with the same names.

To export specific VPC configuration items to a CloudFormation template, complete the following steps:

1. **Launch the VPC Export wizard**.
2. **Select a restore point and VPCs to export**.
3. **Specify an IAM identity for export**.
4. **Specify an Amazon S3 bucket where the Cloud Formation template must be placed**.
5. **Specify a reason for the export**.
6. **Finish working with the wizard**.
Step 1. Launch VPC Export Wizard

To launch the VPC Export wizard, complete the following steps.

1. Navigate to Protected Data > VPC.

2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.

3. Click Export > Selected items.
Step 2. Select Restore Point

At the **Export List** step of the wizard, select the VPC configuration items you want to export and a restore point that will be used to export the selected VPC configuration items. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can export the VPC configuration data to an earlier state.

1. To select the restore point:
   a. In the **Choose restore point** section, click the link to the right of **Restore point**.
   b. In the **Available restore points** window, select the necessary restore point and click **Apply**.

2. To select the VPC configuration items:
   a. In the **Create export list** section, select the type of VPC configuration item you want to export and click **Edit**.
   b. In the **Edit export list** window, click **Add to Export List**.
   c. In the **Item List** window, select check boxes next to the items that you want to export, and click **Add**.
   d. In the **Edit export list** window, review the restore list and click **Apply**.

**IMPORTANT**

When performing the export operation, Veeam Backup for AWS does not validate the export list. If any of the VPC configuration items on which the selected items depend are missing from the current VPC configuration, the restore of the selected VPC configuration items from the created CloudFormation template will fail.
Step 3. Specify IAM Identity

At the **Account** step of the wizard, specify an IAM role whose permissions Veeam Backup for AWS will use to perform the export operation.

**IMPORTANT**

Make sure, that the specified IAM role belongs to an AWS account in which you plan to restore the VPC configuration items.

To specify an IAM role for export, select the necessary IAM role from the list.

For an IAM role to be displayed in the IAM Role list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the VPC Restore wizard. To add an IAM role, click **Add** and complete the **Add IAM Role** wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform export. To run the IAM role permission check, click **Check Permissions**. Veeam Backup for AWS will display the **Permission check** window where you can view the progress and results of the performed check. If the IAM role permissions are insufficient, the check will complete with errors. You can view the list of permissions that must be granted to the IAM role in the **Missing Permissions** column.

You can grant the missing permissions to the IAM role in the AWS Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to IAM roles using the AWS Management Console, see **AWS Documentation**.
Step 4. Specify Amazon S3 Bucket

At the **Target** step of the wizard, specify an Amazon S3 bucket where Veeam Backup for AWS will save the CloudFormation template with the exported VPC configuration items.

Choose whether you want to save the template in the root folder of the selected Amazon S3 bucket or to create a new folder for the template.
Step 5. Specify Export Reason

At the **Reason** step of the wizard, specify a reason for the export of the VPC configuration items. The information you provide will be saved in the session history and you can reference it later.
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing Restore

In various disaster recovery scenarios, Veeam Backup for AWS allows you to perform the following restore operations using backed-up data:

- **Restore of EC2 instances** — restore EC2 instances from cloud-native snapshots, snapshot replicas or image-level backups to the original location or to a new location.

- **Restore of RDS resources** — restore DB instances and Aurora DB clusters from cloud-native snapshots, snapshot replicas to the original location or to a new location.

- **Restore of EFS file systems** - restore file systems from backups to the original location or to a new location.

- **Restore of VPC configurations** — restore VPC configurations from VPC configuration backups to the original location or to a new location.
EC2 Restore

Veeam Backup for AWS offers the following restore options:

- **Instance Restore** — restores an entire EC2 instance.
- **Volume Restore** — restores EBS volumes attached to an EC2 instance.
- **File-Level Restore** — restores individual files and folders of an EC2 instance.

You can restore EC2 instance data to the most recent state or to any available restore point.
Performing Entire EC2 Instance Restore

In case of a disaster, you can restore an entire EC2 instance from a cloud-native snapshot, snapshot replica or image-level backup. Veeam Backup for AWS allows you to restore one or more EC2 instances at a time, to the original location or to a new location.

**NOTE**

If you restore multiple EC2 instances that have the same EBS volume attached, Veeam Backup for AWS will restore one volume per each instance and enable the Multi-Attach option for every restored volume. To recover the source configuration, when the restore operation completes, manually delete extra EBS volumes in the AWS Management Console and attach the necessary volume to the instances.

For more information on Amazon EBS Multi-Attach, see AWS Documentation.

How Instance Restore Works

To restore EC2 instances from cloud-native snapshots and snapshot replicas, Veeam Backup for AWS uses native AWS capabilities. To restore EC2 instances from image-level backups, Veeam Backup for AWS performs the following steps:

1. [Applies to archived backups] Retrieves data from the archived restore point.
2. Launches a worker instance in the AWS Region where the restored EC2 instance will reside.
3. Creates empty EBS volumes and attaches them to the worker instance.
   The number of empty EBS volumes equals the number of EBS volumes attached to the backed-up EC2 instance.
4. Restores backed-up data to the empty EBS volumes on the worker instance.
5. Detaches EBS volumes with restored data from the worker instance.
6. Removes the worker instance from Amazon EC2.
7. Creates an EC2 instance in the specified location.
8. Attaches EBS volumes with restored data to the target EC2 instance.
9. [This step applies only if you perform restore to the original location] Powers off the source EC2 instance and removes it from Amazon EC2.

Before You Begin

To restore an EC2 instance from a backup that is stored in an archive repository, you must retrieve the archived data first. You can either retrieve the archived data manually before you begin the restore operation, or launch the data retrieval process right from the Restore wizard. To learn how to retrieve data manually, see Retrieving Data From Archive.

If you plan to restore an EC2 instance to an AWS Outpost, check the following prerequisites:

1. An IAM role you plan to specify for the restore operation must have the following permissions:
   outposts:ListOutposts, outposts:GetOutpostInstanceTypes. To grant the necessary permissions for the IAM role, use the AWS Management Console. For more information on how to grant permissions to an IAM role, see AWS Documentation.
2. If an Outpost subnet is specified in the worker instance network settings, restore of an EC2 instance to an AWS Region to which the AWS Outpost is connected may fail. The issue occurs if the default worker instance type is not supported for the AWS Outpost. To work around the issue, change the default worker profiles as described in Managing Worker Profiles.

### How to Perform Instance Restore

To restore a protected EC2 instance, complete the following steps:

1. Launch the Instance Restore wizard.
2. Select a restore point.
4. Specify IAM identity for restore.
5. Choose a restore mode.
6. Enable encryption for EBS volumes.
7. Specify EC2 instance settings.
8. Configure network settings.
9. Specify a restore reason.
10. Finish working with the wizard.
Step 1. Launch Instance Restore Wizard

To launch the Instance Restore wizard, complete the following steps.

1. Navigate to Protected Data > EC2.

2. Select the EC2 instance that you want to restore.

3. Click Restore > Instance Restore.
   Alternatively, click the link in the Restore Points column. Then, in the Available Restore Points window, select the necessary restore point and click Restore > Instance Restore.
Step 2. Select Restore Point

At the **Instances** step of the wizard, select restore points to be used to perform the restore operation for each added instance. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore an EC2 instance to an earlier state.

**IMPORTANT**

If you select a restore point stored in an archive repository and the same restore point is also available in a standard repository, Veeam Backup for AWS will display the **Confirmation Restore** window. To proceed, choose whether you want to use the archived or standard restore point to perform the restore operation.

To select a restore point:

1. Select the EC2 instance.
2. Click **Restore Point**.
3. In the **Choose restore point** window, select the necessary restore point and click **Apply**.

To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

- **Date** — the date when the restore point was created.
- **Size** — the size of the restore point.
- **Type** — the type of the restore point:
  - **Snapshot** — a cloud-native snapshot created by a backup policy.
  - **Replica** — a snapshot replica created by a backup policy.
  - **Manual Snapshot** — a cloud-native snapshot created manually.
  - **Backup** — an image-level backup created by a backup policy.
  - **Archive** — an archived backup created by a backup policy.
- **State** — the state of the restore point:
  - **Healthy** — the restore point has been verified by the health check session and reported to be healthy.
  - **Incomplete** — the restore point has been verified by the health check session and reported to be corrupted or incomplete.
- **Storage Class** — a storage class of the backup repository where the restore point is stored (for image-level backups).

- **Restore Point Region** — an AWS Region where the restore point is stored (for cloud-native snapshots and snapshot replicas).
- **IAM Role** — an IAM role used to create the restore point (for cloud-native snapshots and snapshot replicas).
Step 3. Specify Data Retrieval Settings

[This step applies only if you have selected to restore from the archived restore point]

At the Data Retrieval step of the wizard, choose a retrieval mode and specify a period for which you want to keep the data available. To do that:

1. In the Retrieval mode section, click the link.
   a. In the Retrieval settings window, for each processed EC2 instance, do the following:
      i. Select an EC2 instance and click Edit.
      ii. In the Edit Retrieval Mode window, select the retrieval mode that Veeam Backup for AWS will use to retrieve the archived data, and click Save. For more information on data retrieval modes, see Retrieving Data From Archive.
   b. To save changes made to the data retrieval settings, click Apply.

2. In the Availability period section, click Edit Availability Period.
   a. In the Availability settings window, specify the number of days for which you want to keep the data available for restore operations. If the time period expires while a restore operation is still running, Veeam Backup for AWS automatically extends the period to keep the retrieved data available for 1 more day. You can also manually extend the availability period later if required.

TIP

If you want to receive an email notification when data availability period is about to expire, select the Send email notification check box and specify the number of hours before data expiration when the notification must be sent.
b. To save changes made to the availability period settings, click **Apply**.
Step 4. Specify IAM Identity

At the Account step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see EC2 Restore IAM Permissions.

IMPORTANT

Make sure that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore EC2 instances.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the IAM role option.
2. Select the necessary IAM role from the list.

For an IAM role to be displayed in the IAM Role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the Instance Restore wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

TIP

To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click Export Missing Permissions.

IMPORTANT

If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Permission check window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

The IAM user must have the following permissions:
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"

NOTE
Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click Recheck.

Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the Temporary access keys option.
2. Use the Access key and Secret key fields to provide the access key ID and the secret access key.
NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 5. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected EC2 instance to the original or to a custom location. If you select the **Restore to new location, or with different settings** option, specify the target AWS Region where the restored EC2 instance will operate.

**IMPORTANT**

To restore to the original location, the IAM role specified at the **Account** step of the wizard must belong to the AWS account where the selected restore point was created.

If you have AWS Outposts in your infrastructure, you can restore EC2 instances to an AWS Outpost. To do that:

1. Select the **Restore to new location, or with different settings** option.
2. From the drop-down list, select the AWS Region to which the AWS Outpost is connected.
3. Click the link to the right of **Select AWS Outpost**.
4. In the **Choose AWS Outpost** window, select the AWS Outpost where you want to restore the selected instances.
5. Click **Apply**.

**NOTE**

Consider the following:

- All objects residing in an AWS Outpost are encrypted.
- An AWS Outpost supports a limited list of instance types.
Step 6. Enable Encryption

[This step applies only if you have selected the **Restore to new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Encryption** step of the wizard, choose whether the restored EBS volumes of the processed EC2 instance must be encrypted with AWS KMS keys:

- If you do not want to encrypt the EBS volumes or want to apply the existing encryption scheme, select the **Use original encryption scheme** option.
- If you want to encrypt the EBS volumes, select the **Restore as encrypted instance** option and choose the necessary KMS key from the **Encryption key** list.

For a KMS key to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at **step 5** and the IAM role specified for the restore operation must have permissions to the key. For more information on KMS keys, see [AWS Documentation](https://aws.amazon.com/documentation/kms/).
Step 7. Specify Instance Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Settings step of the wizard, do the following for each EC2 instance in the list:

1. Select an EC2 instance.
2. If you want to specify a name for the restored EC2 instance, click Rename.
   In the Instance name window, specify the name and click Apply.
3. If you want to change the instance type for the restored EC2 instance, click Edit.
   In the Instance type window, select the necessary instance type and click Apply. For the list of all existing instance types, see AWS Documentation.

**IMPORTANT**

When restoring an EC2 instance, Veeam Backup for AWS uses the original Amazon machine image (AMI) that was used to launch the source instance. If Veeam Backup for AWS cannot find the original AMI, an AMI recommended to launch the restored instance and the Change AMI button are displayed at the Settings step of the wizard. By default, Veeam Backup for AWS recommends an AMI whose configuration is similar to the configuration of the restored instance. However, you can choose another AMI that will be used to perform the restore operation. To do that, click Change AMI and select the necessary AMI in the Instance settings window.
Step 8. Configure Network Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Network step of the wizard, do the following for each EC2 instance in the list:

1. Select an EC2 instance and click Edit.

2. In the Network settings section of the opened window, choose to which Amazon VPC a restored EC2 instance must be connected, select a subnet in which the EC2 instance will be launched and security groups (virtual firewalls) that must be associated with the restored EC2 instance. To select security groups, click Browse to the right of Security group. Then, in the Select Security Group window, add security groups that must be associated with the instance, and click Save.

For a VPC, subnet group and security group to be displayed in the lists of available network specifications, they must be created for the AWS Region specified at step 5 in the AWS Management Console as described in AWS Documentation.

If you restore EC2 instances to the AWS Outpost, for an Outpost subnet to be displayed in the Subnet drop-down list, choose the Amazon VPC that has one or more Outpost subnets.

IMPORTANT

When Veeam Backup for AWS backs up EC2 instances with IPv6 addresses assigned, it does not save the addresses. That is why when you restore these instances, IP addresses are assigned according to the settings specified in AWS for the subnet to which the instances are restored.

3. In the Public IP settings section of the opened window, choose whether you want Veeam Backup for AWS to assign a public IP address to the restored instance.

Related Resources

- What Is Amazon VPC
- VPCs and Subnets
- Security Groups
Step 9. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring EC2 instances. The information you provide will be saved in the session history and you can reference it later.

![Reason step of the wizard](image)

- **Restore reason:**
  - **Reason:**
    - Restoring failed EC2 instances

---

368 | Veeam Backup for AWS | User Guide
Step 10. Finish Working with Wizard

At the Summary step of the wizard, review summary information and click Finish.

**TIP**

If you want to start the restored EC2 instance as soon as the restore process completes, select the Power on target instance after restoring check box.
Performing Volume-Level Restore

In case a disaster strikes, you can restore corrupted EBS volumes of an EC2 instance from a cloud-native snapshot, snapshot replica or image-level backup. Veeam Backup for AWS allows you to restore EBS volumes to the original location or to a new location.

How Volume-Level Restore Works

To restore EBS volumes from cloud-native snapshots and snapshot replicas, Veeam Backup for AWS uses native AWS capabilities. To restore EBS volumes from image-level backups, Veeam Backup for AWS performs the following steps:

1. [Applies to archived backups] Retrieves data from the archived restore point.
2. Launches a worker instance in the AWS Region where the restored EBS volumes will reside.
3. Creates empty EBS volumes and attaches them to the worker instance.
   The number of empty EBS volumes equals the number of volumes you selected to restore.
4. Restores backed-up data to the empty EBS volumes on the worker instance.
5. Detaches EBS volumes with restored data from the worker instance.
6. Removes the worker instance from Amazon EC2.

**NOTE**
Veeam Backup for AWS does not attach restored EBS volumes to any EC2 instances — the volumes are placed to the specified location as standalone EBS volumes.

Before You Begin

To restore an EBS volume from a backup that is stored in the archive backup repository, the archived data must be retrieved first. You can retrieve the archived data manually before you begin the restore operation, or launch data retrieval from the Restore wizard. For more information on data retrieval, see Retrieving Data From Archive.

If you plan to restore EBS volumes to an AWS Outpost, check the following prerequisites:

1. An IAM role you plan to specify for the restore operation must have the following permissions: outposts:ListOutposts, outposts:GetOutpostInstanceTypes. To grant the necessary permissions for the IAM role, use the AWS Management Console.
2. If the Outpost subnet is specified in the worker configuration settings, restore of EBS volumes to an AWS Region to which the AWS Outpost is connected may fail. The issue occurs if the default worker instance type is not supported for the AWS Outpost. In this case, change the default worker profiles as described in Managing Worker Profiles.

How to Perform Volume Restore

To restore EBS volumes attached to a protected EC2 instance, complete the following steps:

1. Launch the Volume Restore wizard.
2. Select a restore point.
3. **Specify data retrieval settings for archived backups.**
4. **Specify IAM identity for restore.**
5. **Choose a restore mode.**
6. **Enable encryption for EBS volumes.**
7. **Specify the restored EBS volume name.**
8. **Specify a restore reason.**
9. **Finish working with the wizard.**
Step 1. Launch Volume Restore Wizard

To launch the **Volume Restore** wizard, complete the following steps.

1. Navigate to **Protected Data > EC2**.
2. Select the EC2 instance whose EBS volumes you want to restore.
3. Click **Restore > Volume Restore**.

   Alternatively, click the link in the **Restore Points** column. Then, in the **Available Restore Points** window, select the necessary restore point and click **Restore > Volume Restore**.
Step 2. Select Restore Point

At the **Instances** step of the wizard, select restore points to be used to perform the restore operation for each added instance. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore EBS volumes to an earlier state.

**IMPORTANT**

If you select a restore point stored in an archive repository and the same restore point is also available in a standard repository, Veeam Backup for AWS will display the **Confirmation Restore** window. To proceed, choose whether you want to use the archived or standard restore point to perform the restore operation.

To select a restore point:

1. Select the EC2 instance.
2. Click **Restore Point**.
3. In the **Choose restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

   - **Date** — the date when the restore point was created.
   - **Size** — the size of the restore point.
   - **Type** — the type of the restore point:
     - **Snapshot** — a cloud-native snapshot created by a backup policy.
     - **Replica** — a snapshot replica created by a backup policy.
     - **Manual Snapshot** — a cloud-native snapshot created manually.
     - **Backup** — an image-level backup created by a backup policy.
     - **Archive** — an archived backup created by a backup policy.
   - **State** — the state of the restore point:
     - **Healthy** — the restore point has been verified by the health check session and reported to be healthy.
     - **Incomplete** — the restore point has been verified by the health check session and reported to be corrupted or incomplete.
   - **Storage Class** — a storage class of the backup repository where the restore point is stored (for image-level backups).
   - **Restore Point Region** — an AWS Region where the restore point is stored (for cloud-native snapshots and snapshot replicas).
   - **IAM Role** — an IAM role used to create the restore point (for cloud-native snapshots and snapshot replicas).
If you want to restore only specific EBS volumes of the selected EC2 instances, you can exclude the unnecessary disks from the restore process. To do that, click **Exclusions** to open the **Specify exclusions** window, select check boxes next to the volumes that you do not want to restore, and click **Apply**.
Step 3. Specify Data Retrieval Settings

[This step applies only if you have selected to restore from the archived restore point]

At the Data Retrieval step of the wizard, choose a retrieval mode and specify a period for which you want to keep the data available. To do that:

1. In the Retrieval mode section, click the link.
   
a. In the Retrieval settings window, for each processed EC2 instance, do the following:
   
i. Select an EC2 instance and click Edit.
   
   ii. In the Edit Retrieval Mode window, select the retrieval mode that Veeam Backup for AWS will use to retrieve the archived data, and click Save. For more information on data retrieval modes, see Retrieving Data From Archive.

   b. To save changes made to the data retrieval settings, click Apply.

1. In the Availability period section, click Edit Availability Period.
   
a. In the Availability settings window, specify the number of days for which you want to keep the data available for restore operations. If the time period expires while a restore operation is still running, Veeam Backup for AWS automatically extends the period to keep the retrieved data available for 1 more day. You can also manually extend the availability period later if required.

   TIP

   If you want to receive an email notification when data is about to expire, select the Send email notification check box and specify the number of hours before data expiration when the notification must be sent.
b. To save changes made to the availability period settings, click **Apply**.
Step 4. Specify IAM Identity

At the Account step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see EC2 Restore IAM Permissions.

**IMPORTANT**
Make sure, that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore EBS volumes.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the IAM role option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the IAM role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the Volume Restore wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

   **TIP**
   To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click Export Missing Permissions.

   **IMPORTANT**
   If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Permission check window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

   The IAM user must have the following permissions:
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"

NOTE
Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click Recheck.

Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the Temporary access keys option.

2. Use the Access key and Secret key fields to provide the access key ID and the secret access key.
**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.

The keys are used to perform this operation only. They are not saved or stored. To learn what permissions are required for performing the operation, see the User Guide.
Step 5. Choose Restore Mode

At the Restore Mode step of the wizard, choose whether you want to restore the selected EBS volumes to the original or to a custom location. If you select the Restore to new location, or with different settings option, specify the AWS Region and Availability Zone to which Veeam Backup for AWS will place the restored EBS volumes.

**IMPORTANT**

To restore to the original location, the IAM role specified at the Account step of the wizard must belong to the AWS account where the selected restore point was created.

If you have AWS Outposts in your infrastructure, you can restore EBS volumes to an AWS Outpost. To do that:

1. Select the Restore to new location, or with different settings option.
2. From the region drop-down list, select the AWS Region to which the AWS Outpost is connected.
3. From the Availability zone drop-down list, select the Availability Zone that the AWS Outpost is homed to.
4. Click the link to the right of Select AWS Outpost.
5. In the Choose AWS Outpost window, select the AWS Outpost where you want to restore EBS volumes of the selected instances.
6. Click Apply.

**NOTE**

Consider the following:

- All objects residing in an AWS Outpost are encrypted.
- An AWS Outpost supports a limited list of EBS volume types. If the type of the restored EBS volume is not supported in the selected AWS Outpost, the restore operation will fail.
Step 6. Enable Encryption

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Encryption step of the wizard, choose whether the restored EBS volumes must be encrypted with AWS KMS keys:

- If you do not want to encrypt the EBS volumes or want to apply the existing encryption scheme, select the **Use original encryption scheme** option.
- If you want to encrypt the EBS volumes, select the **Restore as encrypted volumes** option and choose the necessary KMS key from the Encryption key list.

For a KMS key to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 5 and the IAM role specified for the restore operation must have permissions to the key. For more information on KMS keys, see [AWS Documentation](https://aws.amazon.com/documentation/kms/).
Step 7. Specify EBS Volume Name

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Settings step of the wizard, you can specify a name for each restored EBS volume:

1. Select the necessary EBS volume and click Rename.

2. In the Rename volume window, specify a name for the restored EBS volume and click Apply.

![Image of the Rename volume window in Veeam Backup for AWS]

### Veeam Backup for AWS

**Configure restore settings**

For each restored volume, specify a new name.

- **Instance**: V Hurtado
- **Volume**: —
- **Data Protection**: —

<table>
<thead>
<tr>
<th>Instance</th>
<th>Volume</th>
<th>Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>albor-坂戸-aborrestore-</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>albor-坂戸-aborrestore2-</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>albor-amatoz2-</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>albor-坂戸-aborrestore-</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>albor-坂戸-aborrestore-</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>albor-坂戸-aborrestore-</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>albor-坂戸-aborrestore-</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>albor-坂戸-aborrestore-</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

**Rename volume**

- **Name**: abor-02

![Apply and Cancel buttons]

- **Apply**
- **Cancel**
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring EBS volumes. The information you provide will be saved in the session history and you can reference it later.
## Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

### Volume Restore

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reason:</strong></td>
</tr>
<tr>
<td><strong>Restore mode:</strong></td>
</tr>
<tr>
<td><strong>Location name:</strong></td>
</tr>
</tbody>
</table>

**IAM role:** Default Backup Restore

**User-2019**

- **Restore point:** 09/14/2021 3:00:22 PM
- **Location name:** EU Central (Frankfurt)
- **Disk name:** user-2019

**User-ami0a2**

- **Restore point:** 09/14/2021 3:00:27 PM
- **Location name:** EU Central (Frankfurt)
- **Disk name:** ami-0a2

**Encryption settings**

- Encryption: Encrypted volume
- Encryption key: amrK88
Performing File-Level Restore

In case a disaster strikes, you can recover corrupted or missing files of an EC2 instance from a cloud-native snapshot or image-level backup. Veeam Backup for AWS allows you to download the necessary files and folders to a local machine or restore the files and folders to the source EC2 instance using the file-level recovery browser.

**IMPORTANT**

You can restore files and folders from the following file systems:

- Microsoft Windows systems — FAT, FAT32, NTFS.
- Linux systems — ext2, ext3, ext4, XFS, Btrfs.

Veeam Backup for AWS supports file-level restore only for Microsoft Windows basic volumes.

### How EC2 File-Level Restore Works

To recover files and folders of a backed-up EC2 instance, Veeam Backup for AWS performs the following steps:

1. Launches a worker instance in either of the following AWS Regions:
   - To restore files and folders from a cloud-native snapshot or a snapshot replicas, Veeam Backup for AWS launches the worker instance in the AWS Region where the source EC2 snapshot or snapshot replica resides.
   - To restore files and folders from an image-level backup, Veeam Backup for AWS launches the worker instance in the AWS Region where the backup repository with backed-up data resides.

2. Attaches and mounts EBS volumes of the EC2 instance to the worker instance.

   EBS volumes are not physically extracted from the backup — Veeam Backup for AWS emulates their presence on the worker instance. The source backup itself remains in the read-only state.

3. [This step applies only if you perform restore to the original location] Installs the Veeam restore tool to the source EC2 instance.

4. Launches the file-level recovery browser.

   The file-level recovery browser displays the file system tree of the backed-up EC2 instance. In the browser, you select the necessary files and folders to restore.

5. Saves the selected files and folders to the local machine or restores them to the source EC2 instance if the **Additional restore mode** is enabled.

6. Unmounts and detaches EBS volumes of the backed-up EC2 instance from the worker instance.

7. [This step applies only if you perform restore to the original location] Removes the Veeam restore tool from the source EC2 instance if the **Keep the restore tool at the target instance** option is not selected.

8. Removes the worker instance from Amazon EC2.

### Before You Begin

To recover files and folders of an EC2 instance from a backup that is stored in the archive backup repository, you must retrieve the archived data manually before you begin the file-level recovery operation. For more information on data retrieval, see [Retrieving Data From Archive](#).
Before you start file-level restore, check the following prerequisites:

- The machine from which you plan to open the file-level recovery browser must be allowed to access the worker instances over the internet. To enable internet access for a worker instance, update the security group specified in worker instance settings to add an inbound rule for HTTPS traffic on the port 443. To learn how to add rules to security groups, see AWS Documentation.

- If you plan to perform file-level restore to the original location, make sure that:
  - The IAM role attached to the source EC2 instance has permissions to communicate with the SSM.
  - If the source EC2 instance and backup appliance reside in the same AWS account, the IAM role attached to the source EC2 instance has the following permissions: sqs:ListQueues, sqs:GetQueueUrl, kinesis:List*, kinesis:Describe*, kinesis:Get*, sqs:GetQueueAttributes, sqs:ListDeadLetterSourceQueues.
  - If the source EC2 instance and backup appliance reside in different AWS accounts, the IAM role attached to the source EC2 instance has permissions to assume the following role: arn:aws:iam::<service-account-id>:role/veeam_rto_<original-instance-id>, where the <service-account-id> is an AWS ID of the trusted AWS account, <original-instance-id> is an AWS ID of the source EC2 instance.

How to Perform EC2 File-Level Restore

To recover files and folders of a protected EC2 instance, do the following:

1. Launch the EC2 File-level Recovery wizard.
2. Select a restore point.
3. Choose a restore mode.
4. Specify a restore reason.
5. Finish working with the wizard — start a recovery session.
6. Choose files and folders to recover.
7. Stop the recovery session.
Step 1. Launch EC2 File-level Recovery Wizard

To launch the EC2 File-level Recovery wizard, do the following:

1. Navigate to Protected Data > EC2.
2. Select the EC2 instances whose files and folders you want to recover.
3. Click Restore > File-level Recovery.
   
   Alternatively, click the link in the Restore Points column. Then, in the Available Restore Points window, select the necessary restore point and click Restore > File-level Recovery.
Step 2. Select Restore Point

At the **Instances** step of the wizard, select restore points to be used to perform the restore operation for each added instance. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore files and folders of the backed-up EC2 instance to an earlier state.

To select a restore point:

1. Select the EC2 instance.
2. Click **Restore Point**.
3. In the **Specify restore point** window, select the necessary restore point and click **Apply**.

To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

- **Date** — the date when the restore point was created.
- **Size** — the size of the restore point.
- **Type** — the type of the restore point:
  - **Snapshot** — a cloud-native snapshot created by a backup policy.
  - **Replica** — a snapshot replica created by a backup policy.
  - **Manual Snapshot** — a cloud-native snapshot created manually.
  - **Backup** — an image-level backup created by a backup policy.
  - **Archive** — an archived backup created by a backup policy.
- **State** — the state of the restore point:
  - **Healthy** — the restore point has been verified by the health check session and reported to be healthy.
  - **Incomplete** — the restore point has been verified by the health check session and reported to be corrupted or incomplete.
- **Storage Class** — a storage class of the backup repository where the restore point is stored (for image-level backups).
- **Restore Point Region** — an AWS Region where the restore point is stored (for cloud-native snapshots and snapshot replicas).
- **IAM Role** — an IAM role used to create the restore point (for cloud-native snapshots and snapshot replicas).
IMPORTANT

To recover files and folders of an EC2 instance from a restore point that is stored in the archive backup repository of the S3 Glacier or S3 Glacier Deep Archive storage class, you must retrieve the archived data manually before you begin the file-level recovery operation. For more information on data retrieval, see Retrieving Data From Archive.
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, set the **Additional restore mode** toggle to **On** if you want to enable restore of files and folders to the source EC2 instance in the file-level recovery browser. Before you enable the additional restore mode, ensure that the IAM role attached to the source EC2 instance has all the required permissions to perform restore to the original location.

**IMPORTANT**

Consider the following limitations:

- For EC2 instances running Linux OS, restore of files and folders to the original location is supported only for systemd-based distributions.
- For EC2 instances running Windows OS, restore of files and folders to the original location is supported only if Windows Management Framework (WMF) version 5.1 is installed on the processed instances.

To restore files and folders to the source EC2 instance, Veeam Backup for AWS uses Amazon Kinesis Data Streams. Kinesis Data Streams are charged on a per-shard basis. By default, Veeam Backup for AWS specifies for the Kinesis Data Stream 1 shard with data transfer rate equal to 1 MB per second. You can change the number of shards to be used in the stream using the **Restore rate** slider. For more information on Kinesis Data Streams, see **AWS Documentation**.

**TIP**

If you perform file-level restore to the original location for the selected EC2 instance frequently, you can select the **Keep the restore tool at the target instance** check box. In this case, Veeam Backup for AWS will not remove the Veeam restore tool from the EC2 instance, which will reduce the time of future recovery operations.
Step 4. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for recovering files and folders. This information will be saved to the session history and you will be able to reference it later.
Step 5. Start Recovery Session

At the Summary step of the wizard, review summary information and click Finish.

As soon as you click Finish, Veeam Backup for AWS will close the File-level Recovery wizard, start a recovery session and display the FLR Running Sessions window. During the recovery session, Veeam Backup for AWS will launch a worker instance and attach EBS volumes of the processed EC2 instance to it.

**TIP**

If you accidentally close the FLR Running Sessions window, navigate to Protected Data > EC2 and click the link in the File-Level Recovery URL column to open the window again.

In the FLR Running Sessions window you can track the progress of the recovery session. In the URL column of the window, Veeam Backup for AWS will display a link to the file-level recovery browser. You can use the link in either of the following ways:

- Click the link to open the file-level recovery browser on your local machine while the recovery session is running.
- Copy the link, close the FLR Running Sessions window and open the file-level recovery browser on another machine.

**IMPORTANT**

When you click Copy URL, Veeam Backup for AWS copies the following information to the clipboard:

- A link to the file-level recovery browser includes a public DNS name of the worker instance hosting the browser and authentication information used to access the browser.
- A thumbprint of a TLS certificate installed on the worker instance hosting the file-level recovery browser.

To avoid a man-in-the-middle attack, before you start recovering files and folders, check that the certificate thumbprint displayed in the web browser from which you access the file-level recovery browser matches the provided certificate thumbprint.
Step 6. Choose Items to Recover

In the file-level recovery browser, you can find and recover items (files and folders) of the selected EC2 instance. All recovered items are either saved as a single .ZIP archive to the default download directory on a machine from which you access the browser, or restored to the original EC2 instance.

To recover files and folders from a specific folder, follow the steps:

1. On the **Browse** tab, specify files and folders that you want to recover:
   a. Navigate to the folder that contains the files and folders.
   b. In the working area, select check boxes next to the necessary items and click **Add to Restore List**.

2. Switch to the **Restore List** tab, review the list of files and folders, select check boxes next to the items that you want to recover and do the following:
   o To download the selected files and folders to the local machine, click **Download**.
   o To download the selected files and folders to the source EC2 instance, click **Restore > Keep**.
     Veeam Backup for AWS will save the files with the `restored-` prefix to the same directory where the source files are located.
   o To restore the selected files and folders to the source EC2 instance, click **Restore > Overwrite**.
     Veeam Backup for AWS will overwrite the source files.

As soon as you click **Restore**, Veeam Backup for AWS will recover the selected files. You can track the progress and view the results of the restore operation in the **Session Log** section of the **Restore List** tab.
Step 7. Stop Recovery Session

After you finish working with the file-level recovery browser, it is recommended that you stop the recovery session so that Veeam Backup for AWS can unmount and detach EBS volumes of the processed EC2 instance from the worker instance and remove the worker instance from Amazon EC2.

To stop the recovery session, click **Stop recovery session** in the **FLR Running Sessions** window. If you do not perform any actions in the file-level recovery browser for 30 minutes, Veeam Backup for AWS will stop the recovery session automatically.

**TIP**
If you accidentally close the **FLR Running Sessions** window, navigate to **Protected Data > EC2** and click the link in the **File-Level Recovery URL** column to open the window again.

<table>
<thead>
<tr>
<th>Restore Point</th>
<th>URL</th>
<th>Certificate Thumbprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/01/2020 2:00:18 PM</td>
<td><a href="http://ec2-3-101-37-195.us-w">http://ec2-3-101-37-195.us-w</a>...</td>
<td>67F082F5EF375BAF484F5291...</td>
</tr>
<tr>
<td>05/15/2020 12:00:15 PM</td>
<td><a href="http://ec2-3-101-24-75.us-w">http://ec2-3-101-24-75.us-w</a>...</td>
<td>59B670E81BA589AE20EF56B...</td>
</tr>
</tbody>
</table>

394 | Veeam Backup for AWS | User Guide
RDS Restore

In case of a disaster, you can restore a DB instance or an Aurora DB cluster from a cloud-native snapshot, snapshot replica or an AWS snapshot. Veeam Backup for AWS allows you to restore one or more RDS resources at a time, to the original location or to a new location.

How RDS Restore Works

To restore a DB instance from a snapshot, Veeam Backup for AWS performs the following steps using native AWS capabilities:

1. Creates a DB instance in the specified location.
2. Modifies the configuration setting values of the created DB instance.
3. Restores backed-up databases to the restored DB instance.

To restore an Aurora DB cluster from a snapshot, Veeam Backup for AWS performs the following steps using native AWS capabilities:

1. Creates an Aurora DB cluster in the specified location.
2. Restores backed-up databases to the created Aurora DB cluster.
3. Modifies the configuration setting values of the created Aurora DB cluster.
4. In the created Aurora DB cluster, creates all backed-up DB instances (when restoring to the original location) or creates the primary DB instance (when restoring to a new location).
5. Modifies the configuration setting values of each created DB instance.

How to Perform RDS Restore

To restore a protected RDS resource, complete the following steps:

1. Launch the RDS Restore wizard.
2. Select a restore point.
3. Specify an IAM identity for restore.
4. Choose a restore mode.
5. Enable encryption.
6. Configure RDS instance settings.
7. Configure network settings.
8. Specify a restore reason.
9. Finish working with the wizard.
Step 1. Launch RDS Restore Wizard

To launch the RDS Restore wizard, complete the following steps.

1. Navigate to Protected Data > RDS.
2. Select the RDS resource you want to restore.
3. Click Restore.

Alternatively, click the link in the Snapshots column. Then, in the Available Restore Points window, select the necessary restore point and click Restore.
Step 2. Select Restore Point

At the Instances step of the wizard, you can add DB instances and Aurora DB clusters to the restore session and select restore points to be used to perform restore for each added RDS resource.

By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore an RDS resource to an earlier state.

To select a restore point, do the following:

1. Select the DB instance or Aurora DB cluster, and click Restore Point.
2. In the Choose restore point window, select the necessary restore point and click Apply.

To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

- **Date** — the date when the restore point was created.
- **Size** — the size of the restore point.
- **Type** — the type of the restore point:
  - *Snapshot* — a cloud-native snapshot created by a backup policy.
  - *Replica* — a snapshot replica created by a backup policy.
  - *AWS Snapshot* — an Amazon DB snapshot created in AWS.

**IMPORTANT**

If you select a restore point of the AWS snapshot type, you will not be able to restore an RDS resource to the original location.

- **Restore Point Region** — an AWS Region where a restore point is stored (for cloud-native snapshots and snapshot replicas).
Step 3. Specify IAM Identity

At the Account step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see RDS Restore IAM Permissions.

**IMPORTANT**

Make sure that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore the selected RDS resources.

**Specifying IAM Role**

To specify an IAM role for restore:

1. Select the IAM role option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the IAM role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the RDS Restore wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.

It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

**TIP**

To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click Export Missing Permissions.

**IMPORTANT**

If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Permission check window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

   The IAM user must have the following permissions:
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"

NOTE
Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click Recheck.

Specifying One-Time Access Keys
To specify one-time access keys for restore:

1. Select the Temporary access keys option.
2. Use the Access key and Secret key fields to provide the access key ID and the secret access key.
NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected RDS resources to the original or to a custom location. If you select the **Restore to new location, or with different settings** option, specify the target AWS Region where the restored DB instances and Aurora DB clusters will operate.

Limitations and Requirements

Before you choose the restore mode, consider the following limitations:

- Restore of RDS resources to the original location is not supported if the IAM role specified for the restore operation belongs to an AWS account that differs from the AWS account where the source resources belong.

- Restore of RDS resources to the original location is not supported using restore points of the **AWS snapshot** type — you can restore these resources only to a new location.

- Restore of Aurora multi-master clusters is not supported if the source region differs from the target region specified for the restore operation. However, you can restore these clusters to the source region in the same or in another AWS account. To specify an AWS account in which the clusters will be restored, select an IAM role that belongs to the necessary account at **step 3**.

  Mind that restore of Aurora multi-master clusters using restore points of the **AWS snapshot** type is supported only to the source region within the same AWS account.

- For the Africa (Cape Town), Asia Pacific (Hong Kong), Europe (Milan) and Middle East (Bahrain) regions, mind the following:

  - Restore of Aurora DB clusters residing in the listed regions to a new location is not supported. However, you can restore these clusters to the original location but with different settings.

  - Restore of Aurora DB clusters to the listed regions is not supported if the source region differs from the target region specified for the restore operation.

- When restoring Aurora global databases, Veeam Backup for AWS restores only primary Aurora DB clusters in the primary AWS Regions; secondary clusters must be created manually in the AWS Management Console after the restore operation completes.

For more information on Amazon Aurora global databases, see **AWS Documentation**.
While restoring to a new location, Veeam Backup for AWS creates only primary DB instances in the restored clusters. Additional writer DB instances (for Aurora multi-master clusters) or Aurora Replicas (for Aurora DB clusters with single-master replication) must be added manually in the AWS Management Console after the restore operation completes. To learn how to add DB instances to Amazon Aurora DB clusters, see AWS Documentation.
Step 5. Enable Encryption

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Encryption step of the wizard, choose whether the restored RDS resources must be encrypted with AWS KMS keys:

- If you do not want to encrypt the RDS resources or want to apply the existing encryption scheme, select the Use original encryption scheme option.
- If you want to encrypt the RDS resources, select the Restore as encrypted instance option and choose the necessary KMS key from the Encryption key list.

For a KMS key to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 4 and the IAM role specified for the restore operation must have permissions to the key. For more information on KMS keys, see AWS Documentation.

**IMPORTANT**

If you plan to restore an unencrypted Aurora provisioned DB cluster to an Aurora Serverless DB cluster, and you select the Use original encryption scheme option, mind that Veeam Backup for AWS will encrypt the newly created Aurora Serverless DB cluster with the default KMS key in the target AWS Region. For more information on Aurora Serverless, see AWS Documentation.
Step 6. Configure Restore Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Settings step of the wizard, specify settings for the restored RDS resources. To do that, follow the instructions provided in sections Configuring Settings for DB Instances and Configuring Settings for Aurora DB Clusters.

**TIP**

The Settings step also contains some preconfigured settings retrieved from the source RDS resources. If you want to specify advanced configuration settings for a restored DB instance or Aurora DB cluster, select the necessary resource and click Advanced Options. For more information on all available settings that can be specified for RDS resources, see the Amazon RDS User Guide and Amazon Aurora User Guide.

Configuring Settings for DB Instances

To configure settings for a restored DB instance, at the Settings step of the wizard, select the necessary instance and click Edit. In the opened window, do the following:

1. In the **Instance identifier** section, specify an identifier for the restored DB instance. Consider the following limitations:
   - The instance identifier must be unique for each AWS Region within one AWS Account.
   - The instance identifier can contain only lowercase Latin letters and hyphens, but cannot contain two consecutive hyphens.
   - The first character of the instance identifier must be a letter. The last character of the identifier must not be a hyphen.
   - The maximum length of the instance identifier is 63 characters.
   For more information on limitations for DB instance identifiers, see AWS Documentation.

2. In the **Instance specifications** section, choose a DB instance class and storage type for the restored instance. If you choose the Provisioned IOPS (SSD) storage type, you must also specify an IOPS rate.
   For the list of all supported DB instance classes and available storage types, see AWS Documentation.

3. In the **Instance options** section, specify a parameter group and an option group that will be associated with the restored instance:
   - a. From the Parameter group drop-down list, select the parameter group containing database engine configuration values that will be applied to the restored DB instance.
     For a parameter group to be displayed in the list of available groups, the group must be created beforehand as described in AWS Documentation.
   - b. [This step does not apply to DB instances running the PostgreSQL database engine] From the Option group drop-down list, select the option group containing database configuration values and security settings that will be applied to the restored DB instance.
     For an option group to be displayed in the list of available groups, the group must be created beforehand as described in AWS Documentation.
NOTE

If you select the **Use default group** option, Veeam Backup for AWS will associate the restored DB instance with the default parameter group and the default option group automatically created by AWS during the restore operation.

4. Click **Apply**.

Configuring Settings for Aurora DB Clusters

A number of settings that you can configure for a restored cluster depends on the capacity type that you plan to choose for the cluster. AWS supports Aurora DB clusters of 2 different capacity types:

- **Aurora provisioned DB cluster** — a cluster whose capacity is managed manually by creating DB instances: a single primary DB instance (writer) and multiple Aurora Replicas (readers) in Aurora DB clusters with single-master replication, and multiple DB instances (writers) in Aurora multi-master clusters. For more information on provisioned DB clusters, see [AWS Documentation](https://aws.amazon.com/documentation/aurora/provisioned/).

- **Aurora Serverless DB cluster** — a clusters whose capacity is scaled automatically according to the specified minimum and maximum capacity values. For more information on Aurora Serverless, see [AWS Documentation](https://aws.amazon.com/documentation/aurora/serverless/).

Before you choose a capacity type for the restored cluster, consider the following limitations:

- Aurora Serverless is supported only for a limited list of AWS Regions and specific DB engine versions. For more information, see [AWS Documentation](https://aws.amazon.com/documentation/aurora/serverless/).

- You can restore an Aurora Serverless DB cluster either as an Aurora Serverless DB cluster or as an Aurora provisioned DB cluster. However, you cannot restore an Aurora provisioned DB cluster as an Aurora Serverless DB cluster unless the source cluster is running the following DB engine versions: MySQL 5.6.10a, MySQL 2.07.1, PostgreSQL 10.12 and PostgreSQL 10.14.
Configuring Settings for Provisioned Cluster

To specify settings for a restored Aurora DB cluster, at the Settings step of the wizard, select the necessary cluster and click Edit. In the opened window, do the following:

1. In the Instance specifications section, specify configuration settings for the restored Aurora DB cluster:
   a. From the Capacity type drop-down list, select Provisioned.

**NOTE**
You cannot change replication settings for restored Aurora DB clusters. Veeam Backup for AWS restores the clusters with the same replication settings configured for the source clusters.

   b. [This step applies only to Aurora MySQL DB clusters with single-master replication and Aurora PostgreSQL DB clusters] Set the Use global database toggle to On if you plan that the restored cluster will have secondary DB clusters in a number of AWS Regions. In this case, the Version list will be filtered to show only Aurora database versions that support this feature. However, Veeam Backup for AWS will still create only a primary cluster in the AWS Region selected at step 4; secondary clusters must be created manually in the AWS Management Console after the restore operation completes.

   For more information on Amazon Aurora global databases, see AWS Documentation.

   c. [This step applies only to Aurora MySQL DB clusters with single-master replication] Set the Use parallel query toggle to On if you plan to use the Aurora MySQL parallel query feature to improve I/O performance and to reduce network traffic in the restored cluster. In this case, the Version list will be filtered to show only Aurora database versions that support this feature. Keep in mind that to be able to use the feature, you must enable the aurora_parallel_query parameter in the DB cluster parameter group that you will specify in the Instance options section.

   For more information on Aurora MySQL parallel query, see AWS Documentation.

   d. From the Version drop-down list, select an Aurora database engine version for the restored cluster. The list shows only DB engine versions supported in the target AWS Region, and is filtered based on the DB engine type and DB engine version of the source Aurora DB cluster. The number of versions displayed in the list also depends on the source cluster replication settings and options that you have selected at steps 1b and 1c.

   For more information on Amazon Aurora database engine versions, see AWS Documentation.

**NOTE**
If you restore Aurora PostgreSQL DB clusters and plan to use the Babelfish feature to allow the restored clusters to accept database connections from Microsoft SQL Server clients, mind that this feature is supported only for Aurora PostgreSQL 13.4 and later engine versions.

   e. In the Cluster identifier field, specify an identifier for the restored cluster. Consider the following limitations:
      - The cluster identifier must be unique for each AWS Region within one AWS Account.
      - The cluster identifier can contain only lowercase Latin letters and hyphens, but cannot contain two consecutive hyphens.
      - The first character of the cluster identifier must be a letter. The last character of the identifier must not be a hyphen.
• The maximum length of the cluster identifier is 63 characters.

For more information on limitations for Aurora DB cluster identifiers, see AWS Documentation.

f. From the **Instance class** drop-down list, select a DB instance class that Veeam Backup for AWS will use to create the primary DB instance in the restored cluster.

For the list of all supported DB instance classes, see AWS Documentation.

**NOTE**

Veeam Backup for AWS supports Aurora Serverless v2. To restore the primary DB instance of the provisioned cluster as an Aurora Serverless v2 DB instance, select *db.serverless* from the **Instance class** drop-down list.

Mind the following limitations:

- **Aurora Serverless v2** is supported only for a limited list of DB engine versions. For more information, see AWS Documentation.
- You cannot specify a capacity range for the restored Aurora Serverless v2 DB instance. If the source DB instance had the same instance class, Veeam Backup for AWS will restore the instance with the backed-up capacity range. Otherwise, Veeam Backup for AWS will restore the Aurora Serverless v2 DB instance with the default capacity range — 8-64 Aurora Capacity Units (ACUs).

g. In the **Instance identifier** field, specify an identifier for the primary DB instance in the restored cluster. Consider the following limitations:

  - The instance identifier must be unique for each AWS Region within one AWS Account.
  - The instance identifier can contain only lowercase Latin letters and hyphens, but cannot contain two consecutive hyphens.
  - The first character of the instance identifier must be a letter. The last character of the identifier must not be a hyphen.
  - The maximum length of the instance identifier is 63 characters.

For more information on limitations for DB instance identifiers, see AWS Documentation.

2. In the **Instance options** section, specify a DB cluster parameter group that will be associated with the restored cluster and a DB parameter group that will be associated with the primary DB instance:

   a. From the **Cluster parameter group** drop-down list, select the DB cluster parameter group containing database engine configuration values that will be applied to every DB instance launched in the restored cluster.

      For a DB cluster parameter group to be displayed in the list, the group must be created beforehand as described in AWS Documentation.

   b. From the **Parameter group** drop-down list, select the DB parameter group containing database engine configuration values that will be applied to the primary DB instance in the restored cluster.

      For a DB parameter group to be displayed in the list, the group must be created beforehand as described in AWS Documentation.

**NOTE**

If Veeam Backup for AWS cannot find any parameter groups in the target AWS Region, the **Use default group option** will be displayed. Use this option to associate the restored DB cluster and the primary DB instance with the default parameter groups that will be automatically created by AWS during the restore operation.
To specify settings for a restored Aurora DB cluster, at the Settings step of the wizard, select the necessary cluster and click Edit. In the opened window, do the following:

1. In the Instance specifications section, specify configuration settings for the restored Aurora DB cluster:
   a. From the Capacity type drop-down list, select Serverless.
   b. From the Version drop-down list, select an Aurora database engine version for the restored cluster. The list shows only DB engine versions supported in the target AWS Region, and is filtered based on the DB engine type and DB engine version of the source Aurora DB cluster.

   For more information on Amazon Aurora database engine versions, see AWS Documentation.

   c. In the Cluster identifier field, specify an identifier for the restored cluster. Consider the following limitations:
      - The cluster identifier must be unique for each AWS Region within one AWS Account.
      - The cluster identifier can contain only lowercase Latin letters and hyphens, but cannot contain two consecutive hyphens.
      - The first character of the cluster identifier must be a letter. The last character of the identifier must not be a hyphen.
      - The maximum length of the cluster identifier is 63 characters.

   For more information on limitations for Aurora DB cluster identifiers, see AWS Documentation.
d. Use the **Minimum capacity unit** and **Maximum capacity unit** fields to specify a range of capacity units that will be used to create scaling rules for the restored cluster. These rules define thresholds for CPU utilization, connections and available memory.

   For more information on capacity units and scaling rules, see [AWS Documentation](https://aws.amazon.com/documentation/amazonrds/).  

2. In the **Instance options** section, specify a DB cluster parameter group containing database engine configuration values that will be applied to the restored cluster.

   For a DB cluster parameter group to be displayed in the Cluster parameter group list, the group must be created beforehand as described in [AWS Documentation](https://aws.amazon.com/documentation/amazonrds/).

   **NOTE**

   If Veeam Backup for AWS cannot find any parameter groups in the target AWS Region, the **Use default group option** will be displayed. Use this option to associate the restored DB cluster with the default DB parameter group that will be automatically created by AWS during the restore operation.

3. Click **Apply**.
Step 7. Configure Network Settings

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Network step of the wizard, configure network and security settings for the restored DB instances and Aurora DB clusters. To do that, select the necessary RDS resource and click Edit. In the opened window, do the following:

1. In the Network settings section, specify network settings for the restored RDS resource:
   - For a restored DB instance, choose an Amazon VPC to which the instance will be connected, a subnet group that will be assigned to the instance, an Availability Zone where the instance will reside, and a port that will be used to access the DB instance. Note that the VPC list shows only Amazon VPCs that include one or more subnet groups.
   - For a VPC and a subnet group to be displayed in the lists of available network specifications, they must be created for the AWS Region specified at step 4 in the AWS Management Console as described in AWS Documentation.

   TIP
   If you want to create a passive secondary replica (standby instance) of the restored DB instance, set the Multi-AZ deployment toggle to On. Keep in mind that Multi-AZ deployments are not supported for instances running MS SQL Server Express and MS SQL Server Web editions. For more information on Multi-AZ deployments, see AWS Documentation.

   - For a restored Aurora provisioned DB cluster, choose an Amazon VPC to which the cluster will be restored, a subnet group that includes at least two subnets created in two different Availability Zones of the AWS Region specified at step 4, an Availability Zone where the primary DB instance will reside, and a port that will be used to access the primary DB instance.

   o For a restored Aurora provisioned DB cluster, choose an Amazon VPC to which the cluster will be restored, a subnet group that includes at least two subnets created in two different Availability Zones of the AWS Region specified at step 4, an Availability Zone where the primary DB instance will reside, and a port that will be used to access the primary DB instance.

   - For a restored Aurora Serverless DB cluster, choose an Amazon VPC to which the cluster will be restored, a subnet group that includes at least two subnets created in two different Availability Zones of the AWS Region specified at step 4, and one or more security groups that will control access to the Aurora DB cluster.

2. [This step applies only to DB instances and Aurora provisioned DB clusters] In the Security settings section, specify security settings to control what IP addresses will be able to connect to databases on the restored RDS resource.

   a. If you want to make the restored RDS resource accessible outside the selected Amazon VPC, set the Public accessible toggle to On. Note that the RDS resource must belong to a public subnet group to become publicly accessible.

   b. To specify security groups that will control access to the RDS resource, do the following:

      i. Click the link in the Security group field.

      ii. In the Select Security Group window, select the necessary groups and click Add. Then, click Save to close the window.
3. Click **Apply**.
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the RDS instance. This information will be saved to the session history and you will be able to reference it later.
Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
EFS Restore

Veeam Backup for AWS offers the following restore options:

- **File System Restore** — restores an entire Amazon EFS file system.
- **File-Level Restore** — restores individual files and folders stored in a file system.

You can restore EFS file system data to the most recent state or to any available restore point.

**IMPORTANT**

You can restore an EFS file system only to the same AWS account where the source file system belongs.
Performing Entire File System Restore

In case of a disaster, you can restore an entire EFS file system from an EFS backup or backup copy. Veeam Backup for AWS allows you to restore one or more EFS file systems at a time, to the original location or to a new location.

How File System Restore Works

To restore an EFS file system from a backup, Veeam Backup for AWS performs the following steps using native AWS capabilities:

1. Creates a file system in the specified location.
2. Modifies the configuration setting values of the created EFS file system.
3. Restores backed-up files and folders to the restored file system.

How to Perform File System Restore

To restore a protected EFS file system, complete the following steps:

1. Launch the EFS Restore wizard.
2. Select a restore point.
3. Specify an IAM identity for restore.
4. Choose a restore mode.
5. Enable encryption for the restored file system.
7. Configure network settings.
8. Specify a restore reason.
9. Finish working with the wizard.
Step 1. Launch EFS Restore Wizard

To launch the **EFS Restore** wizard, complete the following steps.

1. Navigate to **Protected Data > EFS**.
2. Select the EFS file system that you want to restore.
3. Click **Restore > Entire EFS**.

Alternatively, click the link in the **Restore Points** column. Then, in the **Available Restore Points** window, select the necessary restore point and click **Restore > Entire EFS**.
Step 2. Select Restore Point

At the **File System** step of the wizard, you can add file systems to the restore session and select restore points to be used to perform the restore operation for each added EFS file system.

By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore a file system to an earlier state.

To select a restore point, do the following:

1. Select the EFS system and click **Restore Point**.
2. In the **Choose restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

   - **Date** – the date when the restore point was created.
   - **Size** – the size of the restore point.
   - **Type** – the type of the restore point:
     - **EFS backup** – an EFS backup created by a backup policy.
     - **EFS backup copy** – a backup copy created by a backup policy.
     - **Manual backup** – an EFS backup created manually.
   - **Restore Point Region** – an AWS Region where the restore point is stored.
Step 3. Specify IAM Identity

At the **Account** step of the wizard, choose whether you want to **use an IAM role** or **one-time access keys of an IAM user** to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see **EFS Restore IAM Permissions**.

**IMPORTANT**

Make sure that the specified IAM role or one-time access keys belong to an AWS account where the source file system resides.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the **IAM role** option.
2. Select the necessary IAM role from the drop-down list.

   For an IAM role to be displayed in the **IAM role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **EFS Restore** wizard. To add an IAM role, click **Add** and complete the **Add IAM Role** wizard.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click **Check Permissions**. Veeam Backup for AWS will display the **Permission check** window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the **Missing Permissions** column. You can grant the missing permissions to the IAM role using the **AWS Management Console** or instruct Veeam Backup for AWS to do it.

   **TIP**

   To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click **Export Missing Permissions**.

   **IMPORTANT**

   If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see **AWS Documentation**.

To let Veeam Backup for AWS grant the missing permissions:

1. In the **Permission check** window, click **Grant**.
2. In the **Grant permissions** window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click **Apply**.

   The IAM user must have the following permissions:
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"

**NOTE**
Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click **Recheck**.

**Specifying One-Time Access Keys**

To specify one-time access keys for restore:

1. Select the **Temporary access keys** option.

2. Use the **Access key** and **Secret key** fields to provide the access key ID and the secret access key.
**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected EFS file system to the original or to a custom location. If you select the **Restore to a new location, or with different settings** option, specify the target AWS Region where the restored file system will reside.
Step 5. Enable Encryption

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Encryption step of the wizard, choose whether the restored file system must be encrypted with AWS KMS keys:

- If you do not want to encrypt the file system or want to apply the existing encryption scheme, select the Use original encryption scheme option.
- If you want to encrypt the file system, select the Restore as encrypted file system option and choose the necessary KMS key from the Encryption key list.

For a KMS key to be displayed in the list of available encryption keys, it must be stored in the AWS Region selected at step 4 and the IAM role specified for the restore operation must have permissions to the key. For more information on KMS keys, see AWS Documentation.
Step 6. Configure General Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Settings step of the wizard, you can specify new names and configuration settings for the restored file system.

To specify a new name, select the file system and click Rename. In the File system name window, specify the name and click Apply.

To specify configuration settings, do the following:

1. Select the file system and click Edit.
2. In the General Settings window, do the following:
   a. From the Storage class availability drop-down list, select one of the following options:
      - Regional — if you want to redundantly store data of the restored file system across all Availability Zones within the selected AWS Region.
      - One Zone — if you want to redundantly store data of the restored file system within a single Availability Zone.
   b. [Applies if you have selected the Regional option] From the Performance mode drop-down list, select a performance mode for the restored file system. For more information on performance modes, see AWS Documentation.
   c. [Applies if you have selected the One Zone option] From the Availability zone drop-down list, select an Availability Zone where the restored file system will be located.
3. To save changes made to the file system settings, click Apply.
Step 7. Configure Network Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Network step of the wizard, configure network and mount target settings for the restored file system.

Choose Virtual Private Cloud

Specify an Amazon VPC to which the restored EFS file system must be connected:

1. In the Network section, click Edit Network Settings.
2. In the Network specifications window, select the necessary Amazon VPC.
   
   For a VPC to be displayed in the VPC list, it must be created in the AWS Management Console for the AWS Region specified at step 4, as described in AWS Documentation.
3. Click Apply.

Configure Mount Targets

Configure settings for mount targets that will be created for the restored file system:

1. Click the link in the Mount targets section.
2. In the Mount targets specification window, click Add.
3. In the Add Mount Target window, do the following:
   a. From the Availability zone drop-down list, select an Availability Zone where the mount target will be created.
   b. From the Subnet drop-down list, select a subnet to which the mount target will be connected.
      
      For a subnet to be displayed in the Subnet list, it must be created for the selected Availability Zone in the AWS Management Console as described in AWS Documentation.
   c. In the IP address section, choose one of the following options:
      
      ▪ Automatic — if you want an IP address to be automatically assigned to the mount target.
      ▪ Static — if you want to specify a static IP address for the mount target.
   d. Add security groups to control inbound and outbound access to the restored file system. To do that, from the Security groups drop-down list, select a security group that will be associated with the mount target and click Add. Note that you cannot add more than 5 security groups.
      
      For a security group to be displayed in the Security groups list, it must be created in the AWS Management Console as described in AWS Documentation.
   e. To save the mount target configuration, click Add.
4. To save the changes made to the mount target settings, click **Apply**.
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the EFS file system. The information you provide will be saved in the session history and you can reference it later.
Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing File-Level Restore

In case a disaster strikes, you can recover corrupted or missing files of an EFS file system from an EFS backup or backup copy. Veeam Backup for AWS allows you to restore files and folders to the original file system or to another file system.

How EFS File-Level Restore Works

To recover files and folders of a backed-up file system using specific file paths, Veeam Backup for AWS sends an API request to AWS to restore the specified files to the selected file system.

To recover files and folders of a backed-up file system using specific file paths, Veeam Backup for AWS performs the following steps:

1. On the backup appliance, restores the EFS index associated with the specified restore point.
2. Launches the file-level recovery browser.
   The file-level recovery browser displays the file system tree of the backed-up EFS file system. In the browser, you select the necessary files and folders to restore.
3. Creates a new EFS directory `aws-backup-restore_<datetime>` in the root directory of the selected file system and restores the specified backed-up files and folders to the created directory.

How to Perform EFS File-Level Restore

To recover files and folders of a protected file system, do the following:

1. Launch the EFS File-level Recovery wizard.
2. Choose a restore type.
3. Configure restore settings.
4. Specify an IAM identity for restore.
5. Choose a restore mode.
6. Specify a restore reason.
7. Finish working with the wizard.
8. Open the file-level recovery browser.
9. Select a restore point.
10. Choose files and folders to recover.
11. Stop the recovery session.
Step 1. Launch EFS File-level Recovery Wizard

To launch the EFS File-level Recovery wizard, do the following:

1. Navigate to Protected Data > EFS.

2. Select the file system whose files and folders you want to recover, and click Restore > File-level Recovery. Alternatively, click the link in the Restore Points column. Then, in the Available Restore Points window, select the necessary restore point and click Restore > File-level Recovery.
Step 2. Choose Restore Type

At the **Restore Type** step of the wizard, choose whether you want to specify the exact paths to files and folders that you want to recover, or to select specific files and folders in the file-level recovery browser.

**IMPORTANT**

If you select the **Browse files** option, Veeam Backup for AWS will launch the EFS FLR session after you complete the **EFS File-level Recovery** wizard. Depending on the number of files stored in the file system, this session can consume up to 4 GB of RAM on the backup appliance.
Step 3. Configure Restore Settings

[This step applies only if you have selected the Specify file paths option at the Restore Type step of the wizard]

At the Restore List step of the wizard, do the following:

1. Specify a restore point that will be used to restore the selected items.
2. Specify files and folders that you want to recover.
Step 2.1 Select Restore Point

By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore files and folders to an earlier state.

To select a restore point:

1. In the **Restore point** section of the **Restore List** step of the wizard, click the link to the right of **Restore point**.
2. In the **Choose restore point** window, select the necessary restore point and click **Apply**.

To help you choose a restore point, Veeam Backup for AWS provides the following information on each available restore point:

- **Date** – the date when the restore point was created.
- **Size** – the size of the restore point.
- **Type** – the type of the restore point:
  - **EFS backup** – an EFS backup created by a backup policy.
  - **EFS backup copy** – a backup copy created by a backup policy.
  - **Manual backup** – an EFS backup created manually.
- **Restore Point Region** – an AWS Region where the restore point is stored.
Step 2.2 Specify Items to Restore

To add files and folders to the restore list:

1. In the Restore list section, click Edit.

2. In the Edit restore list window, do the following:
   a. For each file or folder you want to recover, specify a path in the Item path field and click Add. Note that you cannot add more than 5 paths.
      Paths are case sensitive and cannot contain wild cards and regex strings. The following characters are not supported: ? * : " < > ` .

   b. Review the restore list and click Apply.

NOTE

The specified paths must be related to the mount point of the file system. For example, if the file system is mounted to the /user/mydocs/efs point and the file path is /user/mydocs/efs/file1, specify /file1.
Step 4. Specify IAM Identity

At the Account step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see EFS Restore IAM Permissions.

IMPORTANT
Make sure, that the specified IAM role or one-time access keys belong to an AWS account where the source file system resides.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the IAM role option.
2. Select the necessary IAM role from the drop-down list.
   - For an IAM role to be displayed in the IAM role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the EFS Restore wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.
   - It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

TIP
To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click Export Missing Permissions.

IMPORTANT
If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see AWS Documentation.

To let Veeam Backup for AWS grant the missing permissions:

1. In the Permission check window, click Grant.
2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

   The IAM user must have the following permissions:
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"

**NOTE**
Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click **Recheck**.

---

**Specifying One-Time Access Keys**

To specify one-time access keys for restore:

1. Select the **Temporary access keys** option.

2. Use the **Access key** and **Secret key** fields to provide the access key ID and the secret access key.
NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 5. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore files and folders to the original or to a custom location. If you select the **Restore to new location, or with different settings** option, specify the target AWS Region and the file system to which the files and folders will be restored.
**Step 6. Specify Restore Reason**

At the **Reason** step of the wizard, specify a reason for restoring the files and folders. The information you provide will be saved in the session history and you can reference it later.
Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

[Applies only if you have selected the **Browse files** option at the **Restore Type** step of the wizard] As soon as you click **Finish**, Veeam Backup for AWS will close the **EFS File-level Recovery** wizard, start a recovery session and display the **FLR Running Sessions** window. To select file and folders that you want to recover, follow the instructions provided in steps 7-9.
Step 8. Open FLR Browser

[This step applies only if you have selected the **Browse files** option at the **Restore Type** step of the wizard]

**TIP**

If you accidentally close the **FLR Running Sessions** window, navigate to **Protected Data > EFS** and click the link in the **File-Level Recovery URL** column to open the window again.

In the **FLR Running Sessions** window you can track the progress of the recovery session. In the **URL** column of the window, Veeam Backup for AWS will display a link to the file-level recovery browser. You can use the link in either of the following ways:

- Click the link to open the file-level recovery browser on your local machine while the recovery session is running.
- Copy the link, close the **FLR Running Sessions** window and open the file-level recovery browser on another machine.

**IMPORTANT**

When you click **Copy URL**, Veeam Backup for AWS copies the following information to the clipboard:

- A link to the file-level recovery browser includes a public DNS name or an IP address of the backup appliance hosting the browser and authentication information used to access the browser.
- A thumbprint of a TLS certificate installed on the appliance hosting the file-level recovery browser.

To avoid a man-in-the-middle attack, before you start recovering files and folders, check that the certificate thumbprint displayed in the web browser from which you access the file-level recovery browser matches the provided certificate thumbprint.
Step 9. Select Restore Point

[This step applies only if you have selected the *Browse files* option at the *Restore Type* step of the wizard]

By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore files and folders to an earlier state.

To select a restore point in the file-level recovery browser, do the following:

1. On the **Browse** tab, click the link in the **Restore Point** field.
2. In the **Select Restore Point** window, choose a date when the restore point was created, select the necessary restore point from the **Restore Points** list and click **Apply**.

   The **Restore Points** list shows only restore points that are associated with created EFS indexes.

   **TIP**

   You can search for the necessary files in all indexed restore points simultaneously. To do that, switch to the **Search** tab, specify the file or folder name, its location and click **Search**.

![Select Restore Point](image.png)
Step 10. Choose Items to Recover

[This step applies only if you have selected the **Browse files** option at the **Restore Type** step of the wizard]

In the file-level recovery browser, you can find and recover items (files and folders) of the selected EFS file system. All recovered items are saved to the specified file system.

To select files and folders from the specific folder, do the following:

1. On the **Browse** tab, navigate to the folder that contains the necessary files and folders.
2. In the working area, select check boxes next to the files and folders that you want to restore and click **Add to Restore List**.
3. Repeat steps 1-2 for all other files and folders that you want to restore.
   
   If you want to restore different versions of a specific file or folder, select a new restore point as described in **Step 9. Select Restore Point**, and then repeat steps 1-2.

**TIP**

You can search for the necessary files in all indexed restore points simultaneously. To do that, switch to the **Search** tab, specify the file or folder name, its location and click **Search**.

4. Switch to the **Restore List** tab.
5. On the **Restore List** tab, review the list files and folders, select check boxes next to the items that you want to recover and click **Restore**.

As soon as you click **Restore**, Veeam Backup for AWS will restore the selected files to the file system that you have specified at step 4 of the **EFS File-level Recovery** wizard. You can track the progress and view the results of the restore operation in the **Session Log** section of the **Restore List** tab.
Step 11. Stop Recovery Session

[This step applies only if you have selected the Browse files option at the Restore Type step of the wizard]

After you finish working with the file-level recovery browser, it is recommended that you stop the recovery session. To stop the recovery session, click Stop Recovery Session in the FLR Running Sessions window. If you do not perform any actions in the file-level recovery browser for 30 minutes, Veeam Backup for AWS will stop the recovery session automatically.

**TIP**

If you accidentally close the FLR Running Sessions window, navigate to Protected Data > EFS and click the link in the File-Level Recovery URL column to open the window again.
VPC Configuration Restore

Veeam Backup for AWS offers the following disaster recovery operations:

- **VPC Configuration Restore** — restores an entire VPC configuration.
- **Selected Items Restore** — restores the selected VPC configuration items.

You can restore the VPC configuration data to the most recent state or to any available restore point.

**IMPORTANT**

When restoring VPC route tables, mind that routes that had the **blackhole** state when a restore point was created will not be restored and a restore session will complete with warning. In this case, it is recommended to check the restored target route table configurations in the AWS Management Console to ensure that all traffic flows correctly. To learn how to configure routes in route tables, see [AWS Documentation](#).
Performing Entire Configuration Restore

In case of unexpected configuration changes, you can restore entire Amazon VPC configuration from a VPC configuration backup. Veeam Backup for AWS allows you to restore the VPC configuration to the original location or to a new location.

**IMPORTANT**

Restore to a new location is not supported for the following VPC configuration items:

- Client VPN endpoints.
- Customer gateways and load balancer listeners that use authentication certificates.
- In route tables, for core networks and routes to AWS Outpost local gateways, network interfaces, instances and carrier gateways.

How Entire VPC Configuration Restore Works

To restore the entire VPC configuration from a backup, Veeam Backup for AWS performs the following steps:

1. Retrieves the backed-up VPC configuration from the Veeam Backup for AWS database.
2. Validates the restore operation: sends API requests to AWS to verify that AWS service quotas are not exceeded and there are no subnet CIDR block conflicts.
3. Retrieves information on existing items and their settings in the current Amazon VPC configuration.
4. Restores the backed-up VPC configuration:
   a. Creates the missing VPC configuration items.
   b. Modifies settings of the existing items that do not match the backed-up settings.

How to Perform Entire VPC Configuration Restore

To restore the entire VPC configuration, complete the following steps:

1. Launch the VPC Restore wizard.
2. Select a restore point and VPCs to restore.
3. Specify an IAM identity for restore.
4. Choose a restore mode.
5. Configure mapping for Availability Zones.
7. Specify a restore reason.
8. Finish working with the wizard.
Step 1. Launch VPC Restore Wizard

To launch the VPC Restore wizard, complete the following steps.

1. Navigate to Protected Data > VPC.

2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.

3. Click Restore > Entire VPC.
Step 2. Select Restore Point

At the **Restore List** step of the wizard, select a restore point that will be used to restore the selected VPC configuration. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore the VPC configuration data to an earlier state.

To select a restore point, do the following:

1. In the **Choose restore point** section, click the link to the right of **Restore point**.
2. In the **Available restore points** window, select the necessary restore point and click **Apply**.
3. In the **Choose VPCs to restore** section, select VPCs whose configuration you want to restore.
Step 3. Specify IAM Identity

At the **Account** step of the wizard, choose whether you want to **use an IAM role** or **one-time access keys of an IAM user** to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see **VPC Configuration Restore IAM Permissions**.

**IMPORTANT**

Make sure, that the specified IAM role or one-time access keys belong to an AWS account in which you plan to restore the VPC configuration.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the **IAM role** option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the **IAM role** list, it must be added to Veeam Backup for AWS as described in **Adding IAM Roles**. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the **VPC Restore** wizard. To add an IAM role, click **Add** and complete the **Add IAM Role** wizard.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click **Check Permissions**. Veeam Backup for AWS will display the **Permission check** window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the **Missing Permissions** column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

**TIP**

To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click **Export Missing Permissions**.

**IMPORTANT**

If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see **AWS Documentation**.

To let Veeam Backup for AWS grant the missing permissions:

1. In the **Permission check** window, click **Grant**.
2. In the **Grant permissions** window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click **Apply**.

   The IAM user must have the following permissions:
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click **Recheck**.

### Specifying One-Time Access Keys

To specify one-time access keys for restore:

1. Select the **Temporary access keys** option.
2. Use the **Access key** and **Secret key** fields to provide the access key ID and the secret access key.
NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected VPC configuration to the original or to a custom location. If you select the **Restore to new location, or with different settings** option, specify the target AWS Region where to restore the VPC configuration.

**IMPORTANT**

If you select the **Restore to a new location, or with different settings** option, consider that AWS Regions have different lists of the supported AWS services. VPC endpoints created using an AWS service that is not available in the target AWS Region will not be restored.
Step 5. Configure Availability Zone Mapping

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Availability Zones step of the wizard, for each source Availability Zone, choose an Availability Zone in the target AWS Region to which VPC configuration items of the source Availability Zone will be restored:

1. Choose an Availability Zone from the list and click **Edit Mapping**.

2. In the Map availability zone window, select the target Availability Zone from the **Target region** drop-down list.

3. Click **Apply**.

**IMPORTANT**

The source and target AWS Regions may have different number of Availability Zones. In this case, Veeam Backup for AWS will automatically change subnet configuration for transit gateway VPC attachments, VPC endpoints and load balancers. After restoring, you can modify the subnet configuration manually in the AWS Management Console. To learn how to modify subnet configuration for VPC networking components, see **AWS Documentation**.
Step 6. Review Peering Connection Settings

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Peering Connection** step of the wizard, review preconfigured VPC peering connection settings. You cannot modify the settings for the restored VPC configuration — by default, Veeam Backup for AWS will restore VPC peering connections as follows:

- If you restore both VPCs between which you have created a peering connection, Veeam Backup for AWS will create a peering connection between the restored VPCs in the target AWS Region.

- If you restore a VPC that has a peering connection to a VPC in the same AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the restored VPC in the target AWS Region and the VPC with which the source VPC is peered in the source AWS Region.

- If you restore a VPC that has a peering connection to a VPC in another AWS Region, Veeam Backup for AWS will create an inter-region peering connection between the restored VPC in the target AWS Region and the VPC with which the source VPC is peered in the other AWS Region.

**NOTE**

VPC peering connections will have the **Pending Acceptance** status after restoring. To accept the restored VPC peering connections, use the AWS Management Console. For more information, see [AWS Documentation](#).
Step 7. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring VPC configuration. The information you provide will be saved in the session history and you can reference it later.
Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

<table>
<thead>
<tr>
<th>Restore List</th>
<th>Review configured settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td></td>
</tr>
<tr>
<td>Restore Mode</td>
<td>Restore mode: As a new VPC</td>
</tr>
<tr>
<td>Availability zone</td>
<td>Location name: EU Central (Frankfurt)</td>
</tr>
<tr>
<td>VPC Restore</td>
<td>IAM role name: Default Backup Restore (Default Backup Restore)</td>
</tr>
<tr>
<td>Reason</td>
<td>Reason: Restoring VPC to another region</td>
</tr>
</tbody>
</table>

![VPC Restore configuration](image)
Performing Selected Items Restore

In case of unexpected configuration changes, you can restore only specific items of the Amazon VPC configuration from a VPC configuration backup.

NOTE
If you restore only specific VPC configuration items, you will not be able to choose a location. By default, Veeam Backup for AWS will restore these items to the original location.

How Selected Items Restore Works

To restore specific items of the VPC configuration from a backup, Veeam Backup for AWS performs the following steps:

1. Retrieves from the Veeam Backup for AWS database the backed-up VPC configuration data on items added to a restore list.
2. Validates the restore operation: sends API request to AWS to verify that AWS service quotas are not exceeded and there are no subnet CIDR block conflicts.
3. Retrieves information on existing items and their settings in the current Amazon VPC configuration.
4. Validates the restore list: sends API requests to AWS to check whether any of the selected VPC configuration items depend on other items that are missing from the current VPC configuration.
   In case any VPC configuration items on which the selected items depend are missing, Veeam Backup for AWS allows the user to add the missing items to the restore list.
5. Restores the selected items of the backed-up VPC configuration:
   - Creates the missing VPC configuration items.
   - Modifies settings of the existing items that do not match the backed-up settings.

IMPORTANT
Consider the following:

- VPC peering connections will have the Pending Acceptance status after restoring. To accept the restored VPC peering connections, use the AWS Management Console. For more information, see AWS Documentation.
- If restore of any selected item fails, Veeam Backup for AWS will stop the restore operation and initiate a rollback. During the rollback, Veeam Backup for AWS will delete all newly created items, but will retain all changes made to the existing VPC configuration items.

How to Perform Selected Items Restore

To restore specific items of the VPC configuration, complete the following steps:

1. Launch the VPC Restore wizard.
2. Select a restore point and items to restore.
3. Specify an IAM identity for restore.
4. Specify a restore reason.
5. Finish working with the wizard.
Step 1. Launch VPC Restore Wizard

To launch the VPC Restore wizard, complete the following steps.

1. Navigate to Protected Data > VPC.

2. Select the configuration record for an AWS Region whose VPC configuration you want to restore.

3. Click Restore > Selected Items.
Step 2. Select Restore Point and Items to Restore

At the **Restore List** step of the wizard, select VPC configuration items you want to restore and a restore point that will be used to restore the selected items. By default, Veeam Backup for AWS uses the most recent valid restore point. However, you can restore the VPC configuration data to an earlier state.

1. To select the restore point:
   a. In the **Choose restore point** section, click the link to the right of **Restore point**.
   b. In the **Available restore points** window, select the necessary restore point and click **Apply**.

2. To select the VPC configuration items:
   a. In the **Create restore list** section, click **Edit** and select an Amazon VPC resource that you want to restore.
   b. In the **Edit restore list** window, click **Add to Restore List**.
   c. In the **Item List** window, select check boxes next to the items that you want to restore, and click **Add**.
   d. In the **Edit restore list** window, review the restore list and click **Apply**.
Step 3. Specify IAM Identity

At the Account step of the wizard, choose whether you want to use an IAM role or one-time access keys of an IAM user to allow Veeam Backup for AWS to perform the restore operation. For information on what permissions the IAM role or IAM user must have to perform restore, see VPC Configuration Restore IAM Permissions.

**IMPORTANT**

After you click Next, Veeam Backup for AWS will use the permissions of the specified IAM role or IAM user to validate the restore list created at step 2. If any of the VPC configuration items on which the selected items depend are missing from the current VPC configuration, Veeam Backup for AWS will open the Missing Configuration Items window with the list of the missing items. To proceed to the next step, click Add. The missing items will be automatically added to the restore list.

Specifying IAM Role

To specify an IAM role for restore:

1. Select the IAM role option.
2. Select the necessary IAM role from the list.

   For an IAM role to be displayed in the IAM role list, it must be added to Veeam Backup for AWS as described in Adding IAM Roles. If you have not added the necessary IAM role to Veeam Backup for AWS beforehand, you can do it without closing the VPC Restore wizard. To add an IAM role, click Add and complete the Add IAM Role wizard.

   It is recommended that you check whether the selected IAM role has all the required permissions to perform the operation. If the IAM role permissions are insufficient, the backup policy will fail to complete successfully. To run the IAM role permission check, click Check Permissions. Veeam Backup for AWS will display the Permission check window where you can track the progress and view the results of the check. If the IAM role permissions are insufficient, the check will complete with errors, and the list of permissions that must be granted to the IAM role will be displayed in the Missing Permissions column. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it.

   **TIP**

   To download the full list of missing permissions as a single JSON policy document that you can use to grant the permissions to the role in the AWS Management Console, click Export Missing Permissions.

   **IMPORTANT**

   If your organization uses service control policies (SCPs) to manage permissions in its accounts, and some of the permissions required for the operation are forbidden by these SCPs, Veeam Backup for AWS will not be able to perform the operation even if you grant the permissions to the selected IAM role. For more information on SCPs, see AWS Documentation.

   To let Veeam Backup for AWS grant the missing permissions:

   1. In the Permission check window, click Grant.

   2. In the Grant permissions window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

      The IAM user must have the following permissions:
"iam:CreatePolicy",
"iam:GetRole",
"iam:GetPolicy",
"iam:AttachRolePolicy"

**NOTE**

Veeam Backup for AWS does not store one-time access keys in the configuration database.

3. To make sure that the missing permissions have been successfully granted, click **Recheck**.

**Specifying One-Time Access Keys**

To specify one-time access keys for restore:

1. Select the **Temporary access keys** option.
2. Use the **Access key** and **Secret key** fields to provide the access key ID and the secret access key.
NOTE

Veeam Backup for AWS does not store one-time access keys in the configuration database.
Step 4. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for the restore of VPC configuration items. The information you provide will be saved in the session history and you can reference it later.
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Enabling Data Encryption

For enhanced data security, Veeam Backup for AWS allows you to encrypt backed-up data in backup repositories using Veeam encryption mechanisms. Additionally, Veeam Backup for AWS supports native AWS KMS encryption of EC2 and RDS instance volumes, and cloud-native snapshots.
Backup Repository Encryption

Veeam Backup for AWS allows you to enable encryption at the repository level. Veeam Backup for AWS encrypts backup files stored in backup repositories the same way as Veeam Backup & Replication encrypts backup files stored in backup repositories. To learn what algorithms Veeam Backup & Replication uses to encrypt backup files, see the Veeam Backup & Replication User Guide, section Encryption Standards.

To enable encryption for a backup repository added to the Veeam Backup for AWS infrastructure, configure the repository settings as described in section Adding Backup Repositories and choose whether you want to encrypt data using a password or using a KMS encryption key. After you create a backup policy and specify the backup repository as a target location for EC2 image-level backups or VPC configuration backup copies, as described in sections Creating EC2 Backup Policies and Editing VPC Configuration Backup Policy, Veeam Backup for AWS performs the following steps:

1. Based on the provided password or KMS key, generates an encryption key to protect instance data stored in the backup repository, and stores the key in the configuration database on the backup appliance.
2. Uses the generated key to encrypt backed-up data transferred to the backup repository when running the backup policy.
Veeam Backup for AWS allows you to back up, replicate and restore data of EC2 and RDS instance volumes encrypted with AWS KMS keys. Additionally, you can encrypt unencrypted data and change KMS keys used to encrypt data when performing the following operations:

- Creating EC2 instance snapshot replicas.
- Creating RDS instance snapshot replicas.
- Creating cloud-native snapshots of EC2 instances manually in another location.
- Creating cloud-native snapshots of RDS instances manually in another location.
- Restoring entire EC2 instances to another location.
- Restoring entire RDS instances to another location.
- Restoring EC2 instance volumes to another location.

If you back up, replicate or restore data of an encrypted RDS instance or an EC2 instance that has encrypted EBS volumes, depending on the operation performed with the instance, you must grant to the IAM role that Veeam Backup for AWS uses for the operation permissions to access different KMS keys:

- Creating cloud-native snapshots
- Creating snapshot replicas
- Restoring from cloud-native snapshots
- Creating image-level backups
- Restoring from image-level backups

If you back up, replicate or restore data of an unencrypted RDS instance or EC2 instance, and if you want to encrypt the backed-up or restored data, you must grant to the IAM role that Veeam Backup for AWS uses to perform the operation permissions to access only the KMS key with which you want to encrypt the data.

**NOTE**

To learn how to grant to an IAM role permissions to use a KMS key, see this Veeam KB article.
Creating Cloud-Native Snapshots

The process of creating cloud-native snapshots of an EC2 instance with encrypted EBS volumes and an encrypted RDS instance does not differ from the same process for an instance with unencrypted volumes. The IAM role used to create cloud-native snapshots does not require any additional permissions — Veeam Backup for AWS encrypts these snapshots with the same KMS keys with which the source instance or volume is encrypted.
Creating Snapshot Replicas

The process of creating a snapshot replica of an encrypted RDS instance and an EC2 instance with encrypted EBS volumes differs depending on whether you create snapshot replicas within the same AWS account where the instance resides or not:

- Creating the snapshot replica in the same AWS account where the instance resides.
- Creating the snapshot replica in an AWS account that is different from the AWS account where the instance resides.

Creating Snapshot Replica in Same AWS Account

To create a snapshot replica within the same AWS account where the encrypted EC2 or RDS instance resides, Veeam Backup for AWS performs the following steps:

1. Takes an encrypted cloud-native snapshot of the instance.
2. Copies the created snapshot to the target AWS Region.

To copy the encrypted snapshot, Veeam Backup for AWS uses the IAM role specified at the Targets step of the Add Policy wizard, as described in sections Creating EC2 Backup Policies and Creating RDS Backup Policies. The IAM role must have permissions to access the following KMS keys:

- KMS keys with which data of the source instance is encrypted (source KMS keys).
- A KMS key with which you want to encrypt instance data in the snapshot replica (target KMS key).

**IMPORTANT**

If you do not specify a target KMS key, Veeam Backup for AWS will not create a snapshot replica for the encrypted instance, and the backup session will complete with warnings.
Creating Snapshot Replica in Different AWS Account

The process of creating a snapshot replica differs depending on the AWS resource for what you want to create the snapshot replica:

- Creating the snapshot replica in an AWS account that is different from the AWS account where the EC2 instance resides.
- Creating the snapshot replica in an AWS account that is different from the AWS account where the RDS instance resides.

Creating Snapshot Replica of EC2 Instance

To create a snapshot replica in an AWS account that is different from the AWS account where the EC2 instance with encrypted EBS volumes resides, Veeam Backup for AWS performs the following steps:

1. Takes an encrypted cloud-native snapshot of the EC2 instance.
2. Shares the created snapshot with the target AWS account.
   
   To share the encrypted snapshot, Veeam Backup for AWS uses the IAM role specified at the Sources step of the Add Policy wizard, as described in section Creating EC2 Backup Policies. The IAM role must have permissions to access KMS keys with which EBS volumes of the EC2 instance are encrypted (source KMS keys).

   **IMPORTANT**

   If EBS volumes of the EC2 instance are encrypted with the default key for EBS encryption (aws/ebs alias), Veeam Backup for AWS will not be able to share the snapshot with another AWS account and the replication process will fail. For more information, see this Veeam KB article.

3. Copies the shared snapshot to the target AWS Region in the target AWS account.
   
   To copy the shared encrypted snapshot, Veeam Backup for AWS uses the IAM role specified at the Targets step of the Add Policy wizard, as described in section Creating EC2 Backup Policies. The IAM role must have permissions to access the following KMS keys:

   - The KMS keys with which EBS volumes of the EC2 instance are encrypted (source KMS keys).
   - A KMS key with which you want to encrypt EBS volume data in the snapshot replica (target KMS key).

   **IMPORTANT**

   Note that if you do not specify a target KMS key, Veeam Backup for AWS will not create a snapshot replica for the encrypted instance, and the backup session will complete with warnings.
Creating Snapshot Replica of RDS Instance

To create a snapshot replica in an AWS account that is different from the AWS account where the encrypted RDS instance resides, Veeam Backup for AWS performs the following steps:

1. Takes an encrypted cloud-native snapshot of the RDS instance.
2. Shares the created snapshot with the target AWS account.

To share the encrypted snapshot, Veeam Backup for AWS uses the IAM role specified at the Sources step of the Add Policy wizard, as described in section Creating RDS Backup Policies. The IAM role must have permissions to access a KMS key with which the RDS instance is encrypted (source KMS key).

**IMPORTANT**

If the RDS instance is encrypted with the default encryption key (aws/rds alias), Veeam Backup for AWS will not be able to share the snapshot with another AWS account and the replication process will fail. For more information, see this Veeam KB article.

3. In the target AWS account, copies the shared encrypted snapshot to the same AWS Region where the RDS instance resides in the source AWS account. Then, if the target AWS Region differs from the source AWS Region, copies the shared cloud-native snapshot to the target AWS Region.

To copy the shared encrypted snapshot, Veeam Backup for AWS uses the IAM role specified at the Targets step of the Add Policy wizard, as described in section Creating RDS Backup Policies. The IAM role must have permissions to access the following KMS keys:

- The KMS key with which the RDS instance is encrypted (source KMS key).
- A KMS key with which you want to encrypt RDS instance data in the snapshot replica (target KMS key).

**IMPORTANT**

If you do not specify a target KMS key, Veeam Backup for AWS will not create a snapshot replica for the encrypted instance, and the backup session will complete with warnings.
Restoring From Snapshots and Replicas

The process of restoring an RDS or EC2 instance from an encrypted cloud-native snapshot differs depending on whether you perform restore to the same location where the cloud-native snapshot resides or not:

- Restoring the instance to the same location where the snapshot resides.
- Restoring the instance to another location.

**NOTE**

Consider the following:

- An AWS account in which the cloud-native snapshot resides is also referred to as the source AWS account.
- An AWS account to which you restore the instance is also referred to as the target AWS account.

**Restoring to Same Location**

To restore an EC2 or RDS instance to the location where the snapshot resides, Veeam Backup for AWS uses the IAM role specified for the restore operation, as described in sections *Performing Entire EC2 Instance Restore* and *Performing RDS Instance Restore*. The IAM role must have permissions to access the following KMS keys:

- KMS keys with which the cloud-native snapshot is encrypted.
- A KMS key with which you want to encrypt data of the restored instance.

**Restoring to Another Location**

The process of restoring an instance to another location differs depending on the AWS resource that you want to restore:

- Restoring the EC2 instance to another AWS Region in the same AWS account.
- Restoring the EC2 instance in another AWS account to the same AWS Region.
- Restoring the EC2 instance in another AWS account to another AWS Region.
- Restoring the RDS instance to another AWS Region in the same AWS account.
- Restoring the RDS instance in another AWS account to the same AWS Region.
- Restoring the RDS instance in another AWS account to another AWS Region.

**Restoring EC2 instance in Same AWS Account but to Another AWS Region**

To restore an EC2 instance to another AWS Region in the same AWS account where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Copies the encrypted cloud-native snapshot to the target AWS Region.
2. Creates an EC2 instance in the target AWS Region.
3. Creates encrypted EBS volumes from the copied encrypted snapshot and attaches them to the created EC2 instance.
To copy the encrypted snapshot, and to create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing Entire EC2 Instance Restore. The IAM role must have permissions to access the following KMS keys:

- KMS keys with which the cloud-native snapshot is encrypted (source KMS keys).
- A KMS key with which you want to encrypt EBS volumes of the restored EC2 instance (target KMS key).

### Restoring EC2 Instance to Same AWS Region but in Another AWS Account

To restore an EC2 instance in another AWS account to the same AWS Region where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.

   To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access KMS keys with which the cloud-native snapshot is encrypted (source KMS keys).

   **IMPORTANT**

   According to AWS limitations, cloud-native snapshots encrypted with the default key for EBS encryption (aws/ebs alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default key for EBS encryption, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

2. Creates an EC2 instance in the target AWS account in the same AWS Region where the snapshot resides in the source AWS account.

3. Creates encrypted EBS volumes from the shared encrypted snapshot and attaches them to the created EC2 instance.

   To create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing Entire EC2 Instance Restore. The IAM role must have permissions to access the following KMS keys:

   - The KMS keys with which the cloud-native snapshot is encrypted (source KMS keys).
A KMS key with which you want to encrypt EBS volumes of the restored EC2 instance (target KMS key).

Restoring EC2 Instance to Another AWS Region in Another AWS Account

To restore an EC2 instance to another AWS Region in an AWS account that is different from the AWS account where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.

   To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access the following KMS keys:
   - KMS keys with which the cloud-native snapshot is encrypted (source KMS keys).
   - A KMS key with which you want to encrypt EBS volumes of the restored EC2 instance (target KMS key).

   **IMPORTANT**
   
   According to AWS limitations, cloud-native snapshots encrypted with the default key for EBS encryption (aws/ebs alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default key for EBS encryption, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

2. Copies the shared snapshot to the target AWS Region in the target AWS account.

3. Creates an EC2 instance in the target AWS Region in the target AWS account.

4. Creates encrypted EBS volumes from the shared encrypted snapshot and attaches them to the created EC2 instance.

   To copy the snapshot, create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing Entire EC2 Instance Restore. The IAM role must have permissions to access the following KMS keys:
   - The KMS keys with which the cloud-native snapshot is encrypted (source KMS keys).
The KMS key with which you want to encrypt EBS volumes of the restored EC2 instance (target KMS key).

Restoring RDS Instance to Another AWS Region but in Same AWS Account

To restore an RDS instance to a different AWS Region in the same AWS account where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Copies the encrypted cloud-native snapshot to the target AWS Region.
2. Creates an RDS instance from the copied encrypted snapshot in the target AWS Region.

To copy the encrypted snapshot, and to create the RDS instance, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing RDS Instance Restore. The IAM role must have permissions to access the following KMS keys:

- A KMS key with which the cloud-native snapshot is encrypted (source KMS key).
- A KMS key with which you want to encrypt the restored RDS instance (target KMS key).
Restoring RDS Instance in Another AWS Account but to Same AWS Region

To restore an RDS instance in a different AWS account to the same AWS Region where the cloud-native snapshot resides, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.
   
   To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access a KMS key with which the cloud-native snapshot is encrypted (source KMS key).

   **IMPORTANT**

   According to AWS limitations, cloud-native snapshots encrypted with the default encryption key (aws/rds alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default encryption key, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

2. In the target AWS account, copies the shared snapshot to the same AWS Region where the snapshot resides in the source AWS account, and re-encrypts the snapshot with the KMS keys that you specified to encrypt the restored RDS instance.
   
   To copy the shared encrypted snapshot and to re-encrypt it, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing RDS Instance Restore. The IAM role must have permissions to access the following KMS keys:
   
   - The KMS key with which the cloud-native snapshot is encrypted (source KMS key).
   - A KMS key with which you want to encrypt the restored RDS instance (target KMS key).

3. Creates an encrypted RDS instance from the copied encrypted snapshot in the target AWS account in the same AWS Region where the snapshot resides in the source AWS account.
   
   To create and encrypt the RDS instance, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing RDS Instance Restore. The IAM role must have permissions to access the KMS key with which you want to encrypt the restored RDS instance (target KMS key).
Restoring RDS Instance to Another AWS Region in Another AWS Account

To restore an RDS instance to a different AWS Region in a different AWS account, Veeam Backup for AWS performs the following steps:

1. Shares the encrypted cloud-native snapshot with the target AWS account.
   
   To share the encrypted snapshot, Veeam Backup for AWS uses an IAM role specified in the backup policy settings for creating cloud-native snapshots (if you restore from a snapshot) or for copying and storing snapshot replicas (if you restore from a snapshot replica). The IAM role must have permissions to access the following KMS keys:
   
   - A KMS key with which the cloud-native snapshot is encrypted (source KMS key).
   - A KMS key with which you want to encrypt the restored RDS instance (target KMS key).

   **IMPORTANT**

   According to AWS limitations, cloud-native snapshots encrypted with the default encryption key (aws/rds alias) cannot be shared between AWS accounts. Thus, if the cloud-native snapshot is encrypted with the default encryption key, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.

2. In the target AWS account, copies the shared snapshot to the same AWS Region where the snapshot resides in the source AWS account.
   
   To copy the shared encrypted snapshot, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing RDS Instance Restore. The IAM role must have permissions to access the KMS key with which the cloud-native snapshot is encrypted (source KMS key).

3. Copies the copied encrypted snapshot to the target AWS Region in the target AWS account and re-encrypts the snapshot with the KMS key specified to encrypt the restored RDS Instance.

5. Creates an encrypted RDS instance in the target AWS Region in the target AWS account.
   
   To copy and re-encrypt the snapshot, create and encrypt the RDS instance, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing RDS Instance Restore. The IAM role must have permissions to access the KMS key with which you want to encrypt the restored RDS instance (target KMS key).
Creating Image-Level Backups

The process of creating an image-level backup of an EC2 instance with encrypted EBS volumes differs depending on whether a worker instance processing EBS volume data is launched in the same AWS account or not:

- Creating the image-level backup in the same AWS account where the worker instance is launched.
- Creating the image-level backup in an AWS account that is different from the AWS account where the worker instance is launched.

Creating Image-Level Backup in Same AWS Account

If a worker instance is launched in the same AWS account where the processed EC2 instance resides, Veeam Backup for AWS performs the following steps:

1. Creates an encrypted cloud-native snapshot of the EC2 instance.
2. Creates encrypted EBS volumes from the snapshot, and then attaches them to the worker instance to read and further transfer EBS volume data to a backup repository.

To access the data, Veeam Backup for AWS uses an IAM role specified to launch worker instances, as described in section Configuring Worker Instance Settings. The IAM role must have permissions to access KMS keys with which EBS volumes of the EC2 instance are encrypted (source KMS keys).

Creating Image-Level Backup in Another AWS Account

If a worker instance is launched in an AWS account different from the AWS account where the processed EC2 instance resides, Veeam Backup for AWS performs the following steps:

1. Creates an encrypted cloud-native snapshot of the EC2 instance.
2. Shares the created snapshot with the AWS account where the worker instance is launched.

To share the encrypted snapshot, Veeam Backup for AWS uses the IAM role specified at the Sources step of the Add Policy wizard, as described in section Creating EC2 Backup Policies. The IAM role must have permissions to access KMS keys with which EBS volumes of the EC2 instance are encrypted (source KMS keys).
If EBS volumes of the EC2 instance are encrypted with the default key for EBS encryption (aws/ebs alias), Veeam Backup for AWS will not be able to share the snapshot with another AWS account and the backup process will fail. For more information, see this Veeam KB article.

3. Creates encrypted EBS volumes from the shared encrypted snapshot, and then attaches them to the worker instance to read and further transfer EBS volume data to a backup repository.

   Note that according to AWS requirements, EBS volumes created from encrypted snapshots must also be encrypted. Thus, Veeam Backup for AWS encrypts re-created EBS volumes with the default encryption key specified for the AWS Region where the worker instance is launched.

   To access the data, Veeam Backup for AWS uses an IAM role specified to launch worker instances, as described in section Configuring Worker Instance Settings. The IAM role must have permissions to access the following KMS keys:

   - The KMS keys with which EBS volumes of the EC2 instance are encrypted (source KMS keys).
   - The default encryption key specified for the AWS Region where the worker instance is launched.
Restoring From Image-Level Backups

The process of restoring an EC2 instance with encrypted EBS volumes from an image-level backup differs depending on whether a worker instance is launched in the same AWS account to which you perform restore or not:

- Performing restore from the image-level backup to the AWS account where the worker instance is launched.
- Performing restore from the image-level backup to an AWS account that is different from the AWS account where the worker instance is launched.

**NOTE**

Consider the following:

- An AWS account that owns an IAM role specified for launching worker instances is also referred to as the source AWS account.
- An AWS account to which you restore an instance is also referred to as the target AWS account.
- Veeam Backup for AWS always launches a worker instance in a target AWS Region specified in restore settings. For more information, see Managing Worker Instances.

**Restore to Same AWS Account**

If a worker instance is launched in the same AWS account where the restored EC2 instance will reside, to encrypt EBS volumes of the restored EC2 instance, Veeam Backup for AWS uses an IAM role specified to launch worker instances, as described in section Configuring Worker Instance Settings. The IAM role must have permissions to access to the KMS key with which you want to encrypt EBS volumes of the restored EC2 instance.

**Restore to Another AWS Account**

If a worker instance is launched in an AWS account that is different from the AWS account where the restored EC2 instance will reside, Veeam Backup for AWS performs the following steps:

1. Creates empty EBS volumes in the target AWS Region in the source AWS account and attaches them to the worker instance. To protect data that will be restored to these volumes, Veeam Backup for AWS encrypts the created EBS volumes with the default encryption key specified for the target AWS Region. To encrypt the volumes, Veeam Backup for AWS uses an IAM role specified to launch worker instances, as described in section Configuring Worker Instance Settings. The IAM role must have permissions to access to the default encryption key specified for the target AWS Region in the source AWS account.
2. Restores backed-up data to the empty EBS volumes on the worker instance.
3. Creates an encrypted cloud-native snapshot of the EBS volumes with the restored data.
4. Shares the created snapshot with the target AWS account.

**IMPORTANT**

According to AWS limitations, snapshots encrypted with the default key for EBS encryption (aws/ebs alias) cannot be shared between AWS accounts. Thus, if the default encryption key specified for the target AWS Region in the source AWS account is the default key for EBS encryption, Veeam Backup for AWS will not be able to share the snapshot and the restore process will fail. For more information, see this Veeam KB article.
5. Creates an EC2 instance in the target AWS Region within the target AWS account.

6. Creates encrypted EBS volumes from the shared encrypted snapshot and attaches them to the created EC2 instance.

To create and encrypt EBS volumes, Veeam Backup for AWS uses an IAM role specified for the restore operation, as described in section Performing Entire EC2 Instance Restore. The IAM role must have permissions to access the following KMS keys:

- The default encryption key specified for the target AWS Region in the source AWS account.
- A KMS key with which you want to encrypt EBS volumes of the restored EC2 instance (target KMS key).
Reviewing Dashboard

Veeam Backup for AWS comes with an Overview dashboard that provides at-a-glance real-time overview of the protected AWS resources and allows you to estimate the overall backup performance. The dashboard includes the following widgets:

- **Sessions in Last 24 Hours** — displays the number of sessions started for data protection or disaster recovery operations during the past 24 hours that completed successfully, the number of sessions that completed with warnings, the number of sessions that completed with errors, and the number of sessions that are currently running.

  To get more information on the sessions, click either View Session Logs or any of the widget rows. In the latter case, the Session Logs page will show only those sessions that have the same status as that clicked in the widget.

  For more information on the Session Logs page, see Viewing Session Statistics.

- **Successful Policy Tasks** — displays the number of snapshots, backups and archived backups successfully created by backup policies during a specific time period (the past 24 hours by default).

  To specify the time period, click the link next to the Schedule icon. To get more information on the created snapshots, backups or archived backups, click any of the widget rows. In the latter case, the Session Logs page will show only those sessions during which Veeam Backup for AWS created the same items as that clicked in the widget.

  For more information on the Session Logs page, see Viewing Session Statistics.

- **Protected Workloads** — displays the number of AWS resources that got protected by Veeam Backup for AWS during a specific time period (the past 24 hours by default).

  To specify the time period, click the link next to the Schedule icon. To get more information on the protected resources, click any of the widget rows.

  For more information on the available resources, their properties and the actions you can perform for the resources, see Viewing Available Resources.

- **Storage Usage** — displays the amount of storage space that is currently consumed by restore points created by Veeam Backup for AWS in Amazon S3 buckets. The widget also displays the total amount of storage space used in the S3 Standard, S3 Glacier and S3 Glacier Deep Archive storage classes explicitly.

- **Top Policies** — shows top backup policies for execution time (including retries). For each policy, the widget also calculates the growth rate to detect whether it took less or more time for the policy to complete in comparison with the previous policy run.

- **Bottlenecks Overview** — is designed to help you avoid possible backup bottlenecks.

  The Policy sizing widget verifies whether the appliance CPU and memory resources are enough to process all enabled backup policies and whether the backup policies are sized correctly.

  Note that one backup policy should not protect more than 250 resources for Veeam Backup for AWS to work properly.

  The CPU quota widget analyzes the amount of CPU quota across all regions to detect whether the quota has already been reached in any of the regions, and if Veeam Backup for AWS could not deploy a worker instance in that region during a backup or restore process. For more information on worker profiles, see Managing Worker Profiles.
The **Appliance disk usage** widget analyzes memory usage on the backup appliance, and displays a warning if the memory usage keeps breaching the preconfigured threshold (80%) for 60 minutes in a row. If the problem persists, increase the EBS volume size of the backup appliance or open a support case to remove the unnecessary data from the configuration database.
Viewing Session Statistics

For each performed data protection or disaster recovery operation, Veeam Backup for AWS starts a new session and stores its records in the configuration database. You can track real-time statistics of all running and completed operations on the Session Logs page.

To view the full list of tasks executed during an operation, click the link in the Status column. To view the full list of instances processed during an operation, click the link in the Items column.

TIP

If you want to specify the time period during which Veeam Backup for AWS must keep session records in the configuration database, follow the instructions provided in section Configuring Global Retention Settings.
Collecting Object Properties

You can export properties of objects managed by Veeam Backup for AWS as a single file in the CSV or XML format. To do that, navigate to the necessary tab and click Export. Veeam Backup for AWS will save the file with the exported data to the default download directory on the local machine.

NOTE

Even if you try to export properties of a specific object, Veeam Backup for AWS will still export all properties of all objects present on the currently opened tab.
Updating Veeam Backup for AWS

Veeam Backup for AWS allows you to check for new product versions and available package updates, download and install them from the Web UI.

**NOTE**

If the backup appliance is managed by a Veeam Backup & Replication server, you will not be able to update Veeam Backup for AWS from the Web UI. To learn how to install updates on backup appliances added to the Veeam Backup & Replication infrastructure, see the Integration with Veeam Backup & Replication Guide, section *Upgrading Appliances*.

It is recommended that you timely install available package updates to avoid performance issues while working with the product. For example, timely installed security updates may help you prevent potential security issues and reduce the risk of compromising sensitive data.

- Checking for Updates
- Installing Updates
- Updating IAM Roles
- Viewing Updates History
Checking for Updates

Veeam Backup for AWS automatically notifies you about newly released product versions and package updates available for the operating system running on the backup appliance. However, you can check for available updates manually if required:

1. Switch to the Configuration page.
2. Navigate to Support Information > Updates.
3. Click Check and View Updates.

If new updates are available, Veeam Backup for AWS will display them on the Updates tab of the Veeam Backup for AWS Updater page. To view detailed information on an update, select the check box next to the update and click What’s new?
Installing Updates

To download and install new product versions and available package updates using the Veeam updater service, you can use either of the following options:

- **Install updates immediately**
- **Schedule update installation**

You can also set a reminder to send update notifications.

**IMPORTANT**

Consider the following:

- You can update the standalone backup appliance using the Veeam updater service only. Updating of the backup appliance manually is not supported.
- You can update the backup appliance managed by a Veeam Backup & Replication server from the Veeam Backup & Replication console as described in the Integration with Veeam Backup & Replication Guide, section **Upgrading Appliances**. Updating managed backup appliances using the Veeam updater service is not supported.

To download and install available product and package updates:

1. Open the **Veeam Backup for AWS Updater** page:
   
   a. Switch to the **Configuration** page.
   
   b. Navigate to **Support Information**.
   
   c. On the **Updates** tab, click **Check and View Updates**.

2. On the **Veeam Backup for AWS Updater** page, do the following:
   
   a. In the **Updates are available for this system** section, select check boxes next to the necessary updates.
   
   b. In the **Choose action** section, select the **Install updates now** option, select the **Reboot automatically after install if required** check box to allow Veeam Backup for AWS to reboot the backup appliance if needed, and then click **Install Updates Now**.
NOTE
The updater may require you to read and accept the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.

Veeam Backup for AWS will download and install the updates; the results of the installation process will be displayed on the History tab. Keep in mind that it may take several minutes for the installation process to complete.

NOTE
When installing product updates, Veeam Backup for AWS restarts all services running on the backup appliance, including the Web UI service. That is why Veeam Backup for AWS will log you out when the update process completes.

Scheduling Update Installation
You can instruct Veeam Backup for AWS to automatically download and install available product versions and package updates on a specific date at a specific time:

1. On the Veeam Backup for AWS Updater page, in the Updates are available for this system section, select check boxes next to the necessary updates.

2. In the Choose action section, do the following:
   a. Select the Schedule updates installation option and configure the necessary schedule.
   b. Select the Reboot automatically after install if required check box to allow Veeam Backup for AWS to reboot the backup appliance if needed.

IMPORTANT
When selecting a date and time when updates must be installed, make sure no backup policies are scheduled to run on the selected time. Otherwise, the update process will interrupt the running activities, which may result in data loss.
c. Click **Schedule Updates**.

Veeam Backup for AWS will automatically download and install the updates on the selected date at the selected time; the results of the installation process will be displayed on the **History** tab.

**Setting Update Reminder**

If you have not decided when to install updates, you can set an update reminder — instruct Veeam Backup for AWS to send an update notification later.

To do that, on the **Veeam Backup for AWSUpdater** page, in the **Choose action** section, do the following:

1. Select the **Remind me later** option and choose when you want to receive the reminder.
   - If you select the **Next Week** option, Veeam Backup for AWS will send the reminder next Monday.
2. Click **Remind me later**.
Updating IAM Roles

When you update the backup appliance to a newer version, the improvements and new features instantly become available in Veeam Backup for AWS. However, to meet new requirements, IAM roles must be assigned missing permissions manually either using the Veeam Backup for AWS UI or the AWS Management Console.

Updating Default Backup Restore IAM Role

After every product update, Veeam Backup for AWS checks if the Default Backup Restore IAM role created while installing the solution has all necessary permissions to perform backup and restore operations. If some of the permissions are missing, you will receive a warning in the notification area. For more information on permissions required for the Default Backup Restore IAM role after you update Veeam Backup for AWS to version 4.0, see Full List of IAM Permissions.

You can update the Default Backup Restore IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it:

1. Click the warning.
2. In the IAM Roles Update window, provide one-time access keys of an IAM user that is authorized to update permissions of IAM roles, and then click Apply.

   The IAM user must have the following permissions:

   "iam:CreatePolicy",
   "iam:GetRole",
   "iam:GetPolicy",
   "iam:AttachRolePolicy"

   **NOTE**

   Veeam Backup for AWS does not store one-time access keys in the configuration database.
3. To make sure that the missing permissions have been successfully granted, navigate to Accounts > IAM Roles, select the Default Backup Restore IAM role and click Check AWS Permissions.

Updating Custom IAM Role

To update the custom IAM role, run a permission check for this role at the IAM Roles page as described in section Checking IAM Role Permissions. If some of the permissions are missing, you will receive a warning in the AWS Permission Check window. You can grant the missing permissions to the IAM role using the AWS Management Console or instruct Veeam Backup for AWS to do it. To learn how to grant permissions to IAM roles using the AWS Management Console, see AWS Documentation.
Viewing Updates History

To see the results of the update installation performed on the backup appliance, do the following:

1. Switch to the Configuration page.
2. Navigate to Support Information > Updates.
3. Click Check and view updates.
4. On the Veeam Backup for AWS page, switch to the History tab.

For each date when an update was installed, the Veeam Backup for AWS Updater page will display the name of the update and its status (whether the installation process completed successfully, completed with warnings or failed to complete).

To download logs for the installed updates, select the necessary date in the Date section, and click View Full Log. Veeam Backup for AWS will save the logs as a single file to the default download directory on the local machine.
Getting Technical Support

If you have any questions or issues with Veeam Backup for AWS, you can search for a resolution on Veeam R&D Forums or submit a support case in the Veeam Customer Support Portal.

When you submit a support case, it is recommended that you provide the Veeam Customer Support Team with the following information:

- Version information for the product and its infrastructure components
- The error message or an accurate description of the problem you are facing
- Log files

Viewing Product Details

To view the product details:

1. Switch to the Configuration page.
2. Navigate to Support Information.

The About section of the Updates tab displays the following information:

- Product version — the currently installed version of Veeam Backup for AWS.
- FLR service version — the currently installed version of the File-level recovery service.
- AWS ID — the unique identification number of the AWS account where Veeam Backup for AWS is installed.
- Support ID — the unique identification number of the Veeam support contract.

Downloading Product Logs

To download the product logs, do the following:

1. Switch to the Download Logs tab.
2. Click Download Logs.
3. In the **Download Logs** window, specify a time interval for which logs must be collected:
   
   - Select the **Collect logs for the last** option if you want to collect data for a specific number of days in the past.
   
   - Select the **Collect logs for specified time period** option if you want to collect data for a specific period of time in the past.

4. Click **OK**.

Veeam Backup for AWS will collect logs for the specified time interval and save them to the default download folder on the local machine in a single log.zip archive.
Appendices

This section provides additional information on how to configure AWS endpoints, AWS Identity and Access Management resources required for Veeam Backup for AWS to perform backup and restore operations.
Appendix A. Creating IAM Roles in AWS

You must specify an IAM role for each data protection and disaster recovery operation performed by Veeam Backup for AWS — the solution uses permissions of the specified IAM roles to access AWS services and resources. You can either create an IAM role using Veeam Backup for AWS, or, first create the role in AWS using the AWS Management Console, AWS CLI or AWS API, and then add this role to Veeam Backup for AWS.

This section describes how to create an IAM role for Veeam Backup for AWS using the AWS Management Console. To do that, perform the following steps:

1. Log in to the AWS Management Console using credentials of an AWS account in which you want to create the IAM role.
2. In the AWS services section, navigate to All Services > Security, Identity, & Compliance and click IAM. The IAM console will open.
3. In the IAM console, navigate to Access Management > Roles and click Create role. The Create role wizard will open.
4. At the Trust step of the wizard, do the following:
   - To create the IAM role in the same AWS account where the backup appliance reside, click AWS service. Then, in the Choose a use case section, select EC2 to create the Backup Policy, Service or Restore IAM role or S3 to create the Repository IAM role.
     In this case you must also configure trusted relationships for the created IAM role to allow Veeam Backup for AWS to assume the role.
   - To create the IAM role in another account, click Another AWS account. Then, in the Account ID field, enter the ID of the trusted account — an AWS account where the backup appliance belongs.
     If you want to increase the security of the role, select the Require external ID check box and enter a password. To learn how to use an external ID to increase security of an IAM role, see AWS Documentation.
5. At the Permissions step of the wizard, select an IAM policy that must be attached to the IAM role.
   For an IAM policy to be displayed in the list, it must be created in advance as described in section Appendix B. Creating IAM Policies in AWS.
6. At the Tags step of the wizard, specify AWS tags that will be assigned to the IAM role.
7. At the Review step of the wizard, specify a name and description for the IAM role. Review the configured settings and click Create role.
8. Add the created IAM role to the Veeam Backup for AWS configuration database as described in section Adding IAM Roles.

Configuring Trusted Relationships

After the IAM role is created, configure trust relationships to allow the Veeam Backup for AWS service to use the IAM role for performing operations. To do that:

1. Open the EC2 Management console and navigate to Instances.
2. In the Instances section, locate the EC2 instance running the backup appliance.
3. At the Description tab, click a link to the right of IAM role.
4. On the Summary page, copy the Role ARN — you will need it later.
5. Open the IAM console and navigate to Roles.

6. Click the name of the IAM role for which you want to configure trust relationships.

7. On the Summary page, switch to the Trust relationships tab.

8. Click Edit trust relationship.

9. In the Policy Document field, paste the following:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "<Role ARN>",
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Where <Role ARN> is the ARN that you have copied at step 4.

10. Click Update Trust Policy. Note that it may take up to 5 minutes for AWS to update the trust policy.
Appendix B. Creating IAM Policies in AWS

When you create an IAM role, you must define permissions that the role will have in your AWS infrastructure. To define the role permissions, you must create an IAM policy and attach it to the IAM role. For more information on managing IAM identity permissions, see AWS Documentation.

To create an IAM policy using the AWS Management Console, perform the following steps:

1. Log in to the AWS Management Console using credentials of an AWS account in which you want to create the IAM policy.
2. In the AWS services section, navigate to All Services > Security, Identity, & Compliance and click IAM.
3. In the IAM console, navigate to Access Management > Policies.
4. Click Create policy.
5. Complete the Create policy wizard:
   a. At the Editor step of the , switch to the JSON tab.
   b. Type or paste a JSON policy document.
      The JSON policy document must include permissions required for an IAM role to which you want to attach the policy. For more information on required permissions, see IAM Permissions. To learn how to write JSON policy documents, see AWS Documentation.

   IMPORTANT

   Mind the following AWS limitations on IAM policy sizing:
   - The size of a managed IAM policy cannot exceed 6.144 characters. For more information on managed IAM policies, see AWS Documentation.
   - The total size of inline IAM policies added to an IAM role cannot exceed 10240 characters. For more information on inline IAM policies, see AWS Documentation.

   For more information on IAM character limits, see AWS Documentation.

   c. At the Tags step of the wizard, specify AWS tags that will be assigned to the IAM policy.
   d. At the Review step of the wizard, specify a name and description for the IAM policy. Review the configured settings and click Create policy.

After you create a policy, you can attach it to IAM roles as described in Appendix A. Creating IAM Roles in AWS.
Appendix C. Configuring Endpoints in AWS

If you want worker instances to operate in private environments, that is to use subnets with disabled auto-assignment of Public IPv4 addresses to launch worker instances in AWS Regions, configure specific endpoints for services used by the backup appliance to perform backup and restore operations.

The following interface endpoints are required to perform Veeam Backup for AWS operations.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Interface Endpoints</th>
<th>S3 Gateway Endpoints</th>
</tr>
</thead>
</table>
| Creating EC2 image-level backups | • com.amazonaws.<region>.ec2messages  
• com.amazonaws.<region>.ssm  
• com.amazonaws.<region>.sqs  
• com.amazonaws.<region>.ebs | • com.amazonaws.<region>.s3 |
| EC2 instance restore | • com.amazonaws.<region>.ec2messages  
• com.amazonaws.<region>.ssm  
• com.amazonaws.<region>.sqs | • com.amazonaws.<region>.s3 |
| EC2 volume-level restore | • com.amazonaws.<region>.ec2messages  
• com.amazonaws.<region>.ssm  
• com.amazonaws.<region>.sqs | • com.amazonaws.<region>.s3 |
| EC2 file-level restore from image-level backups | • com.amazonaws.<region>.ec2messages  
• com.amazonaws.<region>.ssm  
• com.amazonaws.<region>.sqs | • com.amazonaws.<region>.s3 |
| EC2 file-level restore from cloud-native snapshots or replicated snapshots | • com.amazonaws.<region>.ec2messages  
• com.amazonaws.<region>.ssm  
• com.amazonaws.<region>.sqs | • com.amazonaws.<region>.s3 |
| EFS indexing | • com.amazonaws.<region>.ssmmessages  
• com.amazonaws.<region>.ssm  
• com.amazonaws.<region>.sqs  
• com.amazonaws.<region>.sts | • com.amazonaws.<region>.s3 |

To create these endpoints, use the specified endpoint names, where <region> is the name of an AWS Region in which worker instances will be launched.

Creating Interface Endpoints

To allow Veeam Backup for AWS to create image-level backups of EC2 instances and to perform restore operations and EFS indexing, configure interface VPC endpoints in AWS regions where worker instances are launched for subnets to which worker instances must be connected. By default, Veeam Backup for AWS uses the default or the most appropriate network settings of AWS Regions to launch worker instances. However, you can add specific worker configurations as described in section Managing Worker Configurations.
For more information on AWS regions in which worker instances are launched to perform specific operations, see Architecture Overview.

To create an interface VPC endpoint, do the following:

1. Log in to the AWS Management Console using credentials of an AWS account in which you want to create the endpoint.
2. In the AWS services section, navigate to All Services > Networking & Content Delivery and click VPC. The VPC console will open.
3. Navigate to Virtual Private Cloud > Endpoints and click Create Endpoint. The Create endpoint wizard will open.
4. At the Endpoint settings step of the wizard, do the following:
   a. [Optional] In the Name tag field, specify a name for the endpoint.
   b. In the Service category section, select AWS services.
5. At the Services step of the wizard, use the following filter Type: Interface and select a service for which you want to create a VPC endpoint.
6. At the VPC step of the wizard, do the following:
   a. From the VPC drop-down list, select a VPC to which the deployed worker instances will be connected.
   b. In the Additional settings section, select the Enable DNS name check box.
7. At the Subnets step of the wizard, select one subnet for each Availability Zone where worker instances will be launched.
8. At the Security groups step of the wizard, select security groups that will be associated with the endpoint network interfaces.
   Ensure that the security group that is associated with the endpoint network interface allows communication between the endpoint network interface and the resources in your VPC that communicate with the service. If the security group restricts inbound HTTPS traffic (port 443) from resources in the VPC, you will not be able to send traffic through the endpoint network interface.
9. At the Policy step of the wizard, select Full access to allow full access to the service. Alternatively, select Custom and attach a VPC endpoint policy that will control permissions on resources available over the VPC endpoint.
10. Click Create Endpoint.

For more information on interface VPC endpoints, see AWS Documentation.

Creating S3 Gateway Endpoints

To allow Veeam Backup for AWS to create image-level backups of EC2 instances, to perform restore operations from these backups, and to save EFS indexes to backup repositories, configure S3 gateway endpoints in AWS regions where worker instances are launched for subnets to which worker instances must be connected. By default, Veeam Backup for AWS uses the default or the most appropriate network settings of AWS Regions to launch worker instances. However, you can add specific worker configurations as described in section Managing Worker Configurations.

For more information on AWS regions in which worker instances are launched to perform specific operations, see Architecture Overview.
To create a gateway endpoint for a subnet, do the following:

1. Log in to the **AWS Management Console** using credentials of an AWS account in which you want to create the endpoint.

2. In the **AWS services** section, navigate to **All Services > Networking & Content Delivery** and click **VPC**. The VPC console will open.

3. Navigate to **Virtual Private Cloud > Endpoints** and click **Create Endpoint**. The **Create endpoint** wizard will open.

4. At the **Endpoint settings** step of the wizard, do the following:
   - [Optional] In the **Name tag** field, specify a name for the endpoint.
   - In the **Service category** section, select **AWS services**.

5. At the **Services** step of the wizard, use the following filter **Type: Gateway** and select `com.amazonaws.<region>.s3`, where `<region>` is a name of an AWS Region in which worker instances will be launched.

6. At the **VPC** step of the wizard, select a VPC to which the deployed worker instances will be connected.

7. At the **Route tables** step of the wizard, select the route tables to be used by the endpoint. AWS automatically will add a route that points traffic destined for the service to the endpoint network interface.

8. At the **Policy** step of the wizard, select **Full access** to allow full access to the service. Alternatively, select **Custom** and attach a VPC endpoint policy that will control permissions on resources available over the endpoint.

9. Click **Create Endpoint**.

For more information on gateway endpoints for Amazon S3, see **AWS Documentation**.

**IMPORTANT**

When you create an S3 gateway endpoint, consider that a VPC and a service for which you create the endpoint must belong to the same AWS Region. That is, when you perform backup operations using endpoints, the processed source instances must reside in the region in which a repository where the backups will be stored is located; when you perform restore operations using endpoints, the instances must be restored to the region in which a repository where the backup files are stored is located.

This limitation is only region-specific - services and VPCs can belong to different AWS accounts.